Exam : 642-642

Title : Quality of Service (QOS)

Ver : 10-04-07

QUESTION 1
Which of the following markers can be set by Committed Access Rate (CAR)? (Choose all that apply.)

A. DSCP bits
B. QoS Group
C. ATM CLP bit
D. Frame Relay DE bit
E. IP precedence bits

Answer: A, B, E

Explanation:

QoS Mechanism	Available markers
Committed Access Rate (CAR)	IP precedence DSCP QoS group MPLS experimental bits
QoS Policy Propagation through BGP (QPPB)	IP precedence QoS group
Policy-based Routing (PBR)	IP precedence QoS group
Class-based Marking	IP precedence DSCP QoS group MPLS experimental bits ATM CLP bit Frame Relay DE bit 802.1Q/ISL cos/priority

Source: Cisco IP QoS Introduction, Page 64

QUESTION 2
What makes the DiffServ model more scalable than the IntServ model? (Choose all that apply.)

A. DiffServ makes use of per-aggregate QoS instead of per-flow QoS.
B. DiffServ makes use of hop-by-hop signaling which allows DiffServ to scale to a larger number of application flows.
C. DiffServ is capable of implementing admission control either locally on the routers or be offloaded to a central policy server using the COPS protocol.
D. DiffServ routers are not compelled to track the state information for each individual flow.

Answer: A, D
Incorrect:
B. No hop-by-hop signaling uses per-hop behavior

C. This is a feature of both models
Sources: Cisco IP QoS Introduction
http://www.cisco.com/en/US/tech/ CK5 43/ CK7 66/technologies_white_paper09186a00800a3e2f.shtml

---

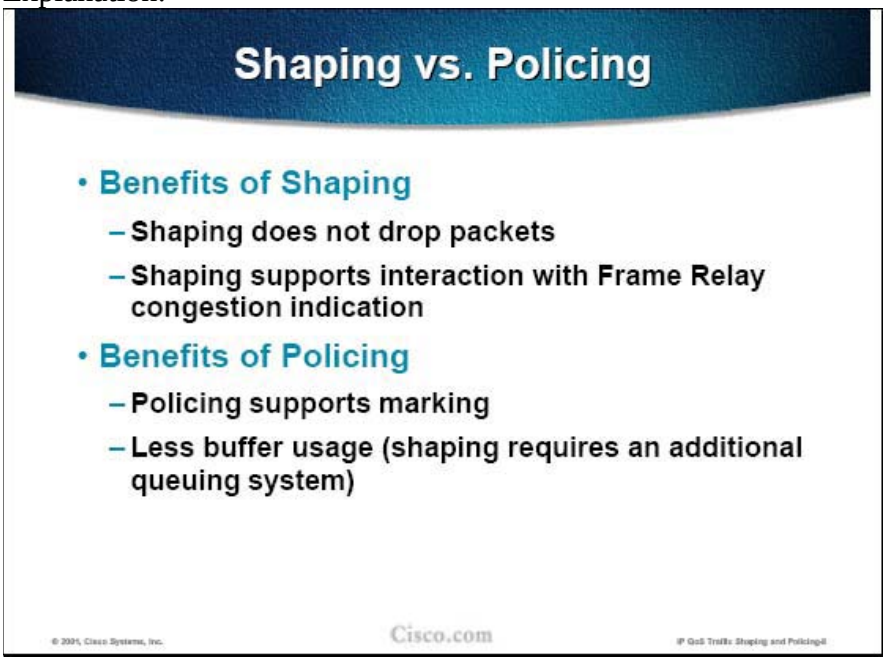
QUESTION 3
The newly appointed Certkiller trainee technician wants to know what the benefits of using traffic shaping to implement network rate limiting is.What will your reply be? (Choose all that apply.)

A. Traffic shaping is an effective tool for rate-limiting VoIP traffic.
B. It will not increase packet loss.
C. It will not add to packet transit delays.
D. Traffic shaping can interact with congestion mechanisms embedded in Frame Relay.
E. Traffic shaping can be used on inbound and outbound traffic on a router.

Answer: B, D
Incorrect:

A. Shaping adds variable delay to traffic, possibly causing jitter
C. A shaper typically delays excess traffic using a buffer
E. This is a feature of policing

Explanation:



Source: Cisco IP QoS Traffic Shaping and Policing

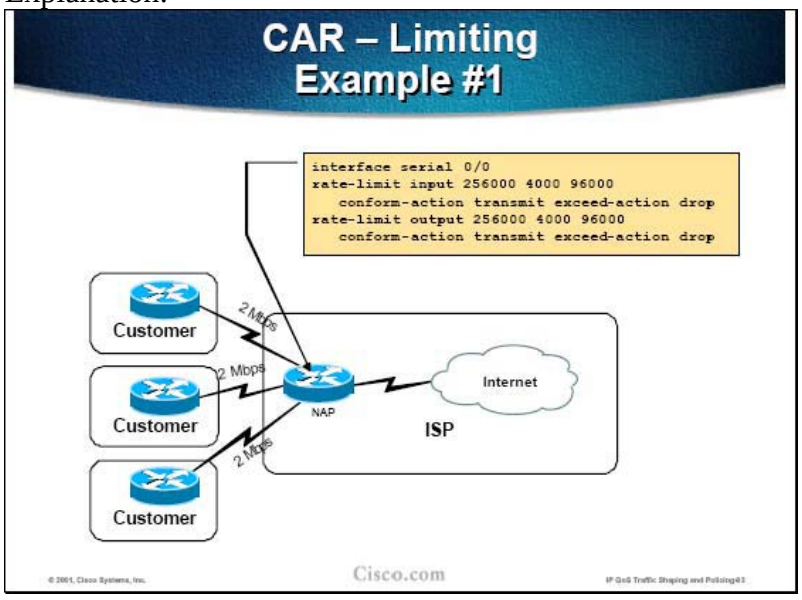
QUESTION 4
Study the Exhibit below carefully:
Router# show interfaces hssi 0/0/0 rate-limit
Hssi0/0/0 45Mbps to R1

Input
matches: all traffic
params: 20000000 bps, 24000 limit, 24000 extended limit
conformed 8 packets, 428 bytes; action: transmit
exceed 0 packets, 0 bytes; action: drop
last packet: 8680ms ago, current burst: 0 bytes
last cleared 00:03:59 ago, conformed 0 bps, exceed 0 bps
Output
matches: all traffic
params: 20000000 bps, 24000 limit, 24000 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceed 0 packets, 0 bytes; action; drop
last packet: 8680ms ago, current burst: 0 bytes
last cleared 00:03:59 ago, conformed 0 bps, exceed 0 bps
According to the exhibit, the router has been configured with Committed Access Rate (CAR) to rate limit traffic.
What data rate has the traffic been limited to?

A. 192 Kbps
B. 2400 Kbps
C. 4,5 Mbps
D. 20 Mbps
E. 40 Mbps

Answer: D

Explanation:



In the configuration example, CAR is applied on the input and output of a customer interface on the provider edge router. Traffic is policed to 256 Kbps on input and output, with some bursting allowed. All exceeding traffic is dropped at the provider edge.
The result of the configuration is that traffic to and from the customer is limited to the

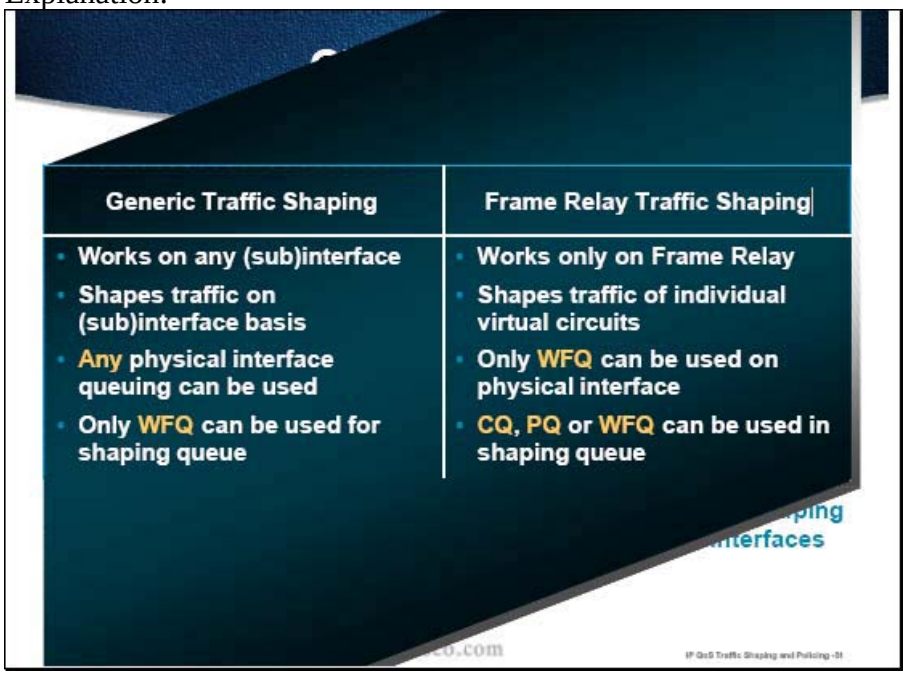
average rate of approximately 256kbps (256000 in the configuration) with sustained bursts of approximately 32kbps (4kBps or 4000 in the configuration).
Initial bursts at line speed can last up to 3 seconds because the token bucket can hold up to 96000 tokens (bytes) which equals 768000 bits (3 x 256000 bits).
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-91

QUESTION 5
The newly appointed Certkiller trainee technician wants to know which type of software queuing mechanism is Frame Relay Traffic Shaping implemented with on the physical interface. What will your reply be?

A. Priority Queuing (PQ)
B. Custom Queuing (CQ)
C. FIFO
D. Weighted Fair Queuing (WFQ)
E. IP Real Time Transport Protocol (RTP) Priority

Answer: D

Explanation:



Works on any (sub) interface type
Shapes traffic on that (sub)interface basis
Can use any physical interface queuing (FIFO, PQ, CQ or WFQ)
Only uses WFQ as the shaping queue (that is, on the input of the shaper)
In contrast, Frame Relay Traffic Shaping:
Works only on Frame Relay (sub) interfaces
Shapes traffic inside individual FR Virtual Circuits
Only permits WFQ as the physical interface queuing method
Can use any queuing method as the shaping queue (that is, on the input of the

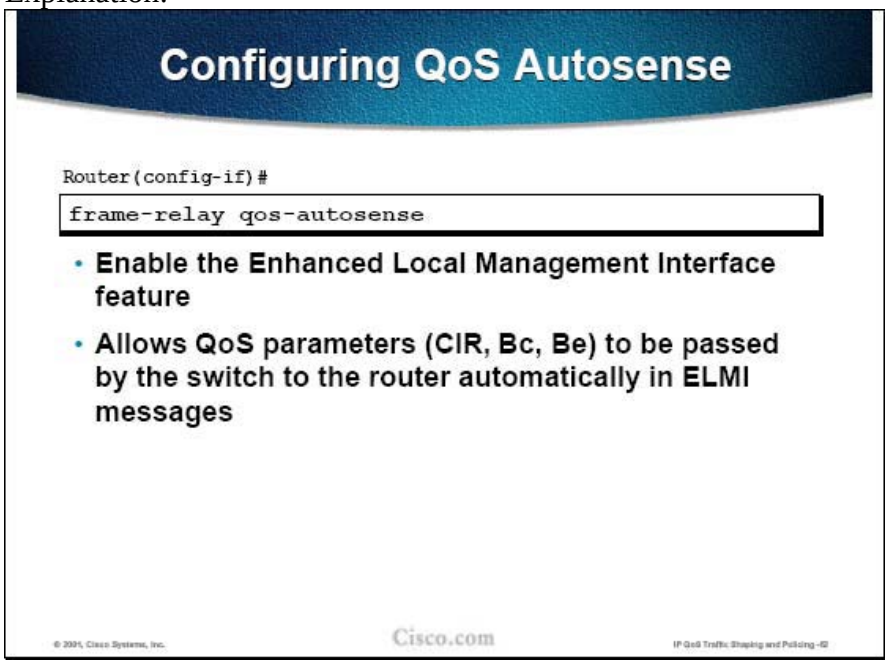
shaper)
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-47

QUESTION 6
Why is it beneficial to make use of Enhanced LMI (ELMI) on Cisco networks?

A. ELMI is responsible for providing virtual provisioning tools at the edge of the Frame Relay network.
B. ELMI permits routers to dynamically download QoS information from Cisco switches for use in traffic shaping or for congestion management purposes.
C. ELMI provides the router the ability to use additional QoS tools including rate limiting with CAR and the Modular QoS Command Line Interface (MQC).
D. ELMI allows the router to deliver packets at the line rate of the Frame Relay interface, regardless of the condition of the Frame Relay network.

Answer: B

Explanation:



Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-58

QUESTION 7
Which of the following statements are true when you compare DSCP and IP Precedence to each other? (Choose all that apply.)

A. DSCP is backwards compatible with IP Precedence.
B.
DSCP cannot be easily mapped into QoS because of its expanded classification options.
C. DSCP is more granular the IP Precedence, since more marking combinations are available.

D. DSCP appears stubby when compared IP Precedence, since devices make use of DSCP as defined in RFC exclusively.
E. DSCP is 6 bits long and IP Precedence is 3 bits long.
F. DSCP is more restrictive than IP Precedence, since devices are only allowed to use DSCP as defined in RFCs.

Answer: A, C, E

Explanation:
A)DSCP is backward compatible with IP Precedence (Class Selector Code point, RFC 1812) but not with the ToS byte definition from RFC 791 ("DTR" bits)
Reference: Introduction to IP QoS (Course) p.45

QUESTION 8
Which MQC command would you use to perform marking properly?

A. precedence 5
B. ip precedence 5
C. set ip precedence 5
D. set ip mark precedence 5
E. mark ip precedence 5

Answer: C

Explanation:
IP precedence is encoded into the three high-order bits of the ToS field in the IP header. It supports eight classes of which two are reserved and should not be used for user-defined classes (IP precedence 6 and 7). IP precedence 0 is the default value and is usually used for the best-effort class. The set ip precedence command marks packets of a class with the specified precedence value.
Reference: Introduction to IP QoS (Course) p.9-104

QUESTION 9
Which of the following statements aptly describes a network well designed for QoS?

A. Packets are classified at each router, based on as many detail as possible, typically using extended IP ACLs to match the packets for classification.
B. Packets are classified at each router, based on socket address only, typically using extended IP ACLs to match the packets for classification.
C. Packets are classified and marked, close to the edge of the network. The packets are treated differently based on this marking at the routers in the middle of the network.
D. Packets are classified based on different parameters, but close to the edge of the network. The packets are automatically characterized based on flow at the routers.
E. Packets are classified based on socket address, at the router closest to the source of the traffic. The packets are automatically characterized based on flow at the routers.

Answer: C

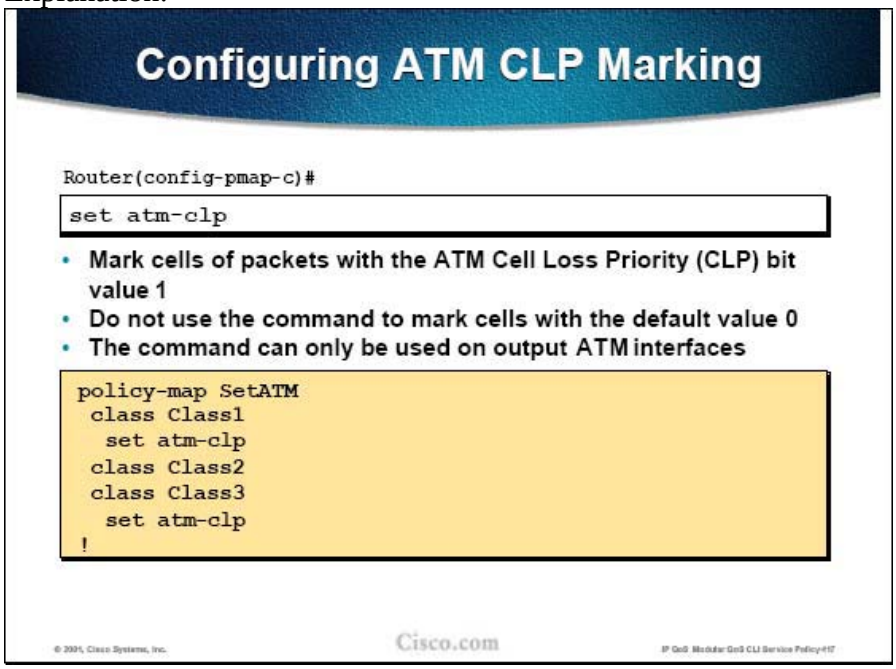
Explanation:
To achieve the same level of quality in both directions the packets going to and coming from the customer network must first be classified and marked.
Classification and marking packets going to the customer network is a more difficult task because:
1) Classifying and marking must be performed on all edge routers.
2) Classifying and marking requires the identification of the customer network. Using PBR, CAR, CB-Policing or CB-Marking does not scale because it involves the use of access lists (this is especially difficult if customer networks are dynamically learned via BGP).
Reference: Introduction to IP QoS (Course) p.2-35

QUESTION 10
The newly appointed Certkiller trainee technician wants to know which bit in the ATM header can be marked by the Class Based Marker to extend IP QoS policy into an ATM network. What will your reply be?

A. DE
B. PTI
C. FECN
D. CLP
E. BECN

Answer: D

Explanation:



The ATM CLP Setting feature somewhat allows users to extend their IP QoS policies

into an ATM network by setting the ATM CLP bit in ATM cells based on the IP Precedence value of the packets being sent. As congestion occurs in the ATM network, cells with the CLP bit set are more likely to be dropped, resulting in improved network performance for high priority traffic and applications. The set
atm-clp
command marks packets of a class with the ATM CLP bit as a part of an input or output policy.
Source: Cisco IP QoS Modular QoS CLI Service Policy, Page 9-110

QUESTION 11
How many possible meaningful values are defined in the DSCP in a Differentiated Services environment?

A. 3
B. 8
C. 16
D. 32
E. 64
F. 128

Answer: E

Explanation:
DSCP supports more classes (64) than IP precedence (8)
Reference: Introduction to IP QoS (Course) p.36

QUESTION 12
Which of the following features will allow the marking of packets according to the Cisco QoS Framework? (Choose all that apply.)

A. MQC
B. CQ
C. PQ
D. CAR
E. WRED

Answer: A, D

Explanation:
The Modular Quality of Service Command Line Interface (MQC) was introduced to allow any supported classification to be used with any QoS mechanism.
Some mechanisms have the capability to mark packets based on classification and/or metering (e.g. CAR, class-based marking, etc.)
Reference: Introduction to IP QoS (Course) p.61

QUESTION 13
Which of the following can be classified as Call Admission Control methods?
(Choose all that apply.)

A. GTS
B. Advanced Busyout Monitor
C. RSVP
D. NBAR
E. Max Connections
F. AVBO.

Answer: C, E, F

Explanation:
http://www.cisco.com/en/US/customer/tech/ CK6 52/ CK7
01/technologies_white_paper09186a00800da467.shtm

QUESTION 14
What are the benefits, as listed in the DQOS course, for Enterprise Networks when
QoS is implemented? (Choose all that apply.)

A. It decreases propagation delay.
B. It provides predictable response times.
C. It prevents the need to increase bandwidth.
D. It supports dedicated bandwidth per application.
E. It maximizes loss during bursty congestion.

Answer: B, D

Explanation:
QoS attemts to solve network traffic performance issues, although QoS is not a cure-all.
To improve network performance, QoS features affect a network by manipulation the
following network characteristics:
1) Bandwidth
2) Delay
3) Jitter (delay variation)
4) Packet loss
Rerference: Cisco Press - DQOS Exam Certification Guide p.9

QUESTION 15
Which of the following is most likely to occur for voice in the absence of QoS?
(Choose all that apply.)

A. choppy speech
B. words out of order due to recovery
C. disconnect calls

D. unsynchronized voice patterns
E. softer volume speech

Answer: A, C

Explanation:
The following most likely occurs for voice in absence of QoS:
Voice is hard to understand; voice breaks up, sounds choppy; calls are disconnected;
large delay make it difficult to know when the other caller has finished talking.
Rerference: Cisco Press - DQOS Exam Certification Guide p.765

QUESTION 16
Auto QoS is which type of Cisco IOS command?

A. interface
B. global
C. policy-map
D. service-map
E. serial interface only

Answer: A

Explanation:
To install the quality-of-service (QoS) class maps and policy maps created by the
AutoQoS for the Enterprise feature, use the auto qos command in interface configuration
mode. To remove the QoS policies, use the no form of this command.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a

---

QUESTION 17
Which two components are associated with the DiffServ model? (Choose two.)

A. hop-by-hop signaling
B. per-hop behavior
C. RSVP
D. Hard QoS
E. DSCP use of class selector

Answer: B, E

Explanation:
The Differentiated Services (DiffServ) model describes services associated with traffic
classes. Traffic classes are identified by the value of the DiffServ Code Point (DSCP
replaces IP precedence in the ToS field of the IP header).
The main goal of the DiffServ model are to provide scalability and a similar level of QoS

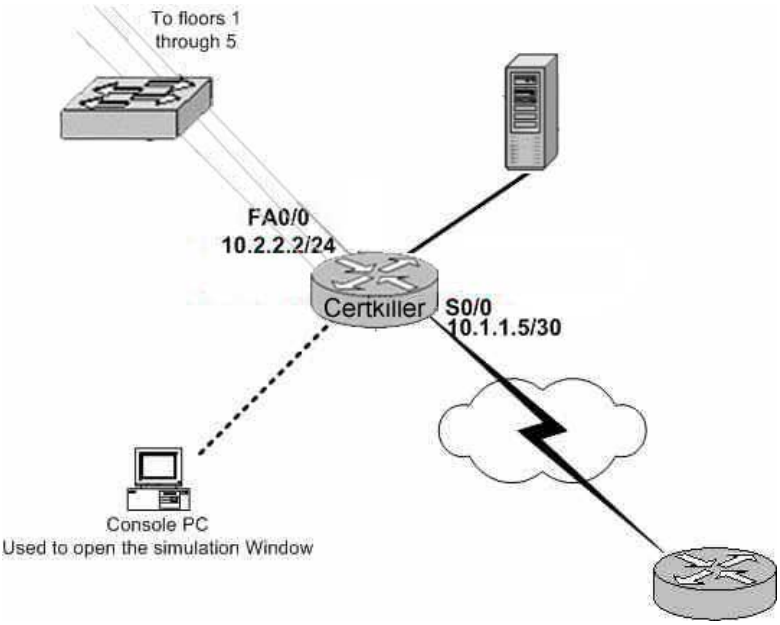
to the Int Serv model, without having to do it on a per-flow basis. The network simply identifies a class (not application) and applies the appropriate per-hop behavior (QoS mechanism)
Reference: Introduction to IP QoS (Course) p.34
Not A: DiffServ does not have signaling

QUESTION 18
What is true about a DSCP marked packet when it reaches an IP precedence based device?

A. The eight DSCP bits are all set to zero.
B. The last three bits of the DSCP are set to 101.
C. The 8 DSCP AF classes will be mapped into the 8 levels of IP precedence.
D. Bits 7-5 of DSCP have the same position and meaning as IP precedence.

Answer: D
Reference: Cisco Press - DQOS Exam Certification Guide p.120

QUESTION 19
SIMULATION
Simulation Exhibit:



You are working as a network administrator at Certkiller .com. You are required to configure the Certkiller 1 WAN edge router: you must configure the appropriate MQC based queuing mechanism for the outbound traffic to the WAN (S0/0) so that the following bandwidth requirements will be met. A strict priority queue with a 168 Kbps bandwidth guarantee for the class voice is reserved, a minimum bandwidth guarantee of 30 Kbps is configured for the class interactive, a minimum bandwidth guarantee of 16 Kbps for class bulk, and the default class is configured for WFQ with no bandwidth guarantee.
In addition, also limit the bulk traffic class to an average rate of 24 Kbps by

buffering excess traffic (use the IOS default Bc and Be).
In addition, also limit the bulk traffic class to an average rate of 24 Kbps by buffering excess traffic (use the IOS default Bc and Be).
* Use a policy-map called "IIq-policy" and reference the existing class-maps already configured on the Certkiller 1 router.
Traffic Class Name Bandwidth Guarantee
voice 168 Kbps maximum (use the IOS default burst value)
interactive 30 Kbps minimum
bulk 16 Kbps minimum (For the bulk traffic class, also limit the traffic to an average rate of 24 Kbps by buffering excess traffic (use the IOS default Bc and Be))
class-default Weighted Fair Queue with no bandwidth guarantee
Simulation Output exhibit #1:

```
Certkiller1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N2 - OSPF NSSA external type 2, N2 - OSPF NSSA external type 2
       N2 - OSPF NSSA external type 2- OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

    10.0.0.0/24   is subnetted, 1 subnets
C      10.2.2.0  is directly connected, FastEthernet0/0
Certkiller1#
Certkiller1#show ip interface brief
Interface              IP-Address       OK? Method Status                Protocol

FastEthernet0/0        10.2.2.2         YES manual   up                    up

FastEthernet0/1        unassigned   YES NVRAM    administratively down down

Serial0/0              10.1.1.5         YES manual   up                    up

Certkiller1#
```

Simulation Output exhibit #2:

Certkiller1#show runn

```
Building configuration...
Current configuration:
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
!
!
logging queue-limit 100
!
ip subnet-zero
!
ip cef
!
!
!
class-map match-any voice
 match ip dscp ef cs3 af31
class-map match-any bulk
 match protocol ftp
 match ip dscp af11
class-map match-any interactive
 match protocol citrix
 match ip dscp af21
!
!
!
!

interface FastEthernet0/1
 ip address 10.2.2.2 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 no ip address
 speed auto
 duplex auto
 shutdown
interface Serial0/0
 bandwidth 384
 ip address 10.1.1.5 255.255.255.252
 encapsulation ppp
!
!
ip http server
ip classless
!
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
```

Answer:
Certkiller 1(config)#policy-map llq-policy
Certkiller 1(config-pmap)#class voice
Certkiller 1(config-pmap-c)#priority 168
Certkiller 1(config-pmap-c)#class interactive
Certkiller 1(config-pmap-c)#bandwidth 30
Certkiller 1(config-pmap-c)#class bulk
Certkiller 1(config-pmap-c)#bandwidth 16
Certkiller 1(config-pmap-c)#shape average 2400
Certkiller 1(config-pmap-c)#class class-default
Certkiller 1(config-pmap-c)#fair-queue
Certkiller 1(config-pmap-c)#interface serial 0/0
Certkiller 1(config-if)#service-policy output llq-policy
Certkiller 1(config-if)#end
Certkiller 1#copy running-config startup-config

Explanation:
policy-map llq-policy (Not: iiq-policy)
shape average 24000 (not shape peak 24(shape in bps not kbps) and shape to average not peak)
Note: Uncertainty:
Actual exam problems:
1. Unable to use the command: fair-queue
Note: There is no need to use the ip nbar protocol-discovery command as the question doesn't state to configure NBAR.

QUESTION 20
Command exhibit: mis qos trust pass-through dscp
Your apprentice Certkiller is configuring a Catalyst 2950 Switch. What is the purpose of the command she is submitting (see exhibit)?

A. The command configures a port to trust the incoming CoS and not modify the incoming DSCP when sending the frame out.
B. The command configures a port to trust the incoming CoS and to generate the internal DSCP based on the incoming CoS. The internalr DSCP will then determine the gress DSCP.
C. The command configures a port to trust the incoming CoS and DSCP values.
D. The command configures a port to trust the incoming CoS and to generate the internal DSCP based on the incoming DSCP. The internal DSCP will then determine the egress DSCP.
E. The command configures a port to trust the incoming CoS and bypass the CoS-to-DSCP maps for generating the internal DSCP.
F. The command configures a port to trust the incoming CoS and bypass the DSCP-to-CoS maps for generating the egress CoS.

Answer: A

Explanation:
When the switch is in pass-through mode, it uses the CoS value of incoming packets without modifying the DSCP value and sends the packets from one of the four egress queues. By default, pass-through mode is disabled. The switch assigns a CoS value of 0 to all incoming packets without modifying the packets. The switch offers best-effort service to each packet regardless of the packet contents or size an dends it from a single egress queue.
To disable pass-through mode, use the no mls qos trust pass-ghrough dscp interface configuration command.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps5213/products_configuration_guide_chapter09186a0

QUESTION 21
Which of the following tasks are necessary when configuring Service Assurance Agent (SAA agent)? (Choose all that apply.)

A. You must schedule the operation
B. You must configure the data collection frequency
C. You must configure the operation type
D. You must configure a collection probe on the router
E. You must configure timer parameters for the SAA agent

Answer: A, C

Explanation:
To configure a new SAA operation, perform the following steps, beginning in in global configuration mode:
Step 1 Enter RTR configuration mode using the rtr op-numbercommand. The op-numberargument specifies an identification number for the operation you will be configuring.
Step 2 Use one of the type commands to specify which type of operation you are configuring.
Step 3 (Optional) Configure characteristics for the operation, one characteristic per line, using the commands found in "Configuring SAA Operation Characteristics" section.
Step 4 Type exit to return to global configuration mode.
Step 5 (Optional) Set reaction conditions for the operation, as explained in the "Reaction Thresholds" section.
Step 6 Schedule the operation start-time, as explained in the "Scheduling the Operation" section.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00

QUESTION 22
The SSA agent is used to measure which of the following SLA metrics? (Choose all that apply.)

A. jitter
B. interface utilization
C. packet loss
D. response time
E. client response
F. router buffer allocation

Answer: A, C, D

Explanation:
The SAA allows you to measure and monitor the following:
SLA metrics such as round-trip response time and availability.
Voice-over-IP (VoIP) metrics such as jitter, packet loss, and availability of synthetic VoIP traffic.
Web metrics and applications.
Quality of Service (QoS) and accuracy metrics such as IP packet precedence levels.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087a78.html

---

QUESTION 23
Which of the following is part of SMS? (Choose all that apply.)

A. QDM
B. CiscoWorks2000 Resource Manager Essentials
C. RSVP COPS Server
D. Service Level Manager
E. CiscoViewCiscoWorks 2000 Management Server
F. All of the above

Answer: B, D, E

Explanation:
SMS includes two main components. First, the Service Level Manager (SLM) is software that runs on the same host as CiscoWorks2000. SLM provides information to the end user of SMS, and generates the configuration of the probes based on end-user input. SMS collection Managers (CMs) are software agents that run on computers spread around the network for scaling purposes, or a CM can reside on the SLM server for small installations.
Reference: Cisco Press - DQOS Exam Certification Guide p.667

QUESTION 24
You are using IP to ATM CoS. Which action can be configured to be automatically taken should a VC in a VC bundle fail?

A. The VC can be remapped to a different bundle.

B. The VC can be declared down and an alternate route requested.
C. The circuit data can be transferred or "bumped" to a lower priority VC.
D. The circuit data can be divided equally between the remaining VCs in the bundle.

Answer: C

Explanation:
In the event of failure, the router responds with one of two methods. The first method dynamically assigns the traffic bound on the failed VC to an alternative VC, which is termed circuit bumping. Bumped traffic is then shared on an existing in-service VC. Traffic typically would be bumped from a higher class to a lower one, although it does not have to be. For example, should the premium, or first class, data circuit become unavailable, then all premium users would share the second class or general circuit. Preference would then be given to the premium traffic within this shared circuit.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800c

---

QUESTION 25
How is IP to ATM CoS supported in a single VC?

A. The IP Precedence bits are mapped into the unused upper bits of the VPI field.
They are treated accordingly as they are switched through the ATM network.
B. The router at the edge of the ATM network sets the ATM CLP based on the IP Precedence bits.
Lower priority packets are transported in lower priority cells.
They are treated accordingly as they are switched through the ATM network.
C. WRED/DWRED is used in the routers at the edge of the ATM network.
Based on the IP Precedence bits, IP traffic is subjected to different drop probabilities (and therefore priorities) as IP traffic coming into a router competes for bandwidth on the ATM VC.
D. PQ-WFQ is used in the routers at the edge of the ATM network.
Based on the IP Precedence bits, IP traffic is then properly queued and de-queued as IP traffic competes for bandwidth on the ATM VC.

Answer: C

Explanation:
Enhanced ATM port adapters (PA-A3) provide the ability to shape traffic on each VC according to the ATM service category and traffic parameters employed. When you use the IP to ATM CoS feature, congestion is managed entirely at the IP layer by WRED running on the routers at the edge of the ATM network.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800c

---

QUESTION 26
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know which LFI mechanism has an option for fragmentation by the Frame Relay DTE, with the switch reassembling the fragments. What will your reply be?

A. FRF .3
B. FRF .9
C. FRF .11 Annex C
D. FRF.12
E. FRF.6

Answer: D

Explanation:
There are three LFI mechanisms implemented in Cisco IOS:
1) Multilink PPP with Interleaving is by far the most common and widely used form of LFI.
2) FRF.12 Frame Relay LFI is used with Frame Relay data connections.
3) In an ATM network, using separate PVC carrying voice and data can be used to interleave packets when they are output on an interface.
Reference: Introduction to IP QoS (course) p.6-47

QUESTION 27
Which of the following statements are valid when considering the need for link efficiency tools such as fragmentation and compression? (Choose all that apply.)

A. Fragmentation allows voice CAC mechanism to increase call volume.
B. While adding bandwidth to counter congestion, reducing load on a link by compression increases available bandwidth.
C. Variable sized packets create extra processing overhead for most IOS queuing mechanism, but fragmentation creates uniformity, thus decreasing queuing delay.
D. Based on link speed, some single packets are large enough that their serialization delay causes intolerable delay for voice or video.
E. All of the above.

Answer: B, D

QUESTION 28
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know in which configuration mode the following MQC command can be used. What will your reply be?
match ip dscp af41?

A. interface configuration mode
B. service policy configuration mode

C. class map configuration mode
D. policy map configuration mode
E. none of the above

Answer: C

Explanation:
Router(config-cmap)#match ip dscp dscp [dcscp ...]
1) Select up to eight DSCP values or names
2) All packets marked with one of the selected DSCP values are matched by this class map.
Reference: Introduction to IP QoS (course) p.8-21

QUESTION 29
What is a key benefit of using the Cisco Modular QoS Command Line Interface (MQC)?

A. Provides performance metrics for QoS configurations.
B. Eliminates the need for map classes to perform traffic classification.
C. Allows users to specify traffic classes independently from QoS polices.
D. Allows QoS policy information to be automatically distributed throughout the network.
E. Provides an integrated testing mechanism for traffic classification and QoS policy configurations.

Answer: C

Explanation:
Modular Quality of Service (QoS) Command-Line Interface (CLI) is a feature that allows users to specify a traffic class independently of QoS policies.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00

QUESTION 30
What is the effect of enabling Weighted Fair Queuing (WFQ) on low-speed router interface?

A. Delay is guaranteed for high-priority traffic types.
B. Bandwidth is guaranteed for different traffic queues.
C. Fixed-size queues are pre-allocated for different traffic flows.
D. Low-bandwidth traffic receives priority over high-bandwidth traffic.

Answer: D

Explanation:
WFQ queuing algorithm should fairly share the bandwidth among flows by:

-reducing response time for interactive flows by scheduling them to the front of the queue
- preventing high volume conversations from monopolizing an interface
Imlementation: Messages are sorted into conversations (flows) and transmitted by the order of the last bit crossing its channel
Unfairness is reinstated by introducing "weight" (IP precedence) to give proportionately more bandwidth to flows with higher weight.
Reference: Introduction to IP QoS p.3-55

QUESTION 31
What is the function of Modular QoS Command Line Interface (MQC) classification?

A. to identify traffic independently of QoS polices
B. to mark traffic based on the Class Latency index (CLI)
C. to route traffic based on the multiple QoS policies
D. to group QoS configuration commands into modules to ease configuration
E. To aggregate traffic onto one QoS classification for operational efficiency (CPU and Memory)

Answer: A

Explanation:
Modular Quality of Service (QoS) Command-Line Interface (CLI) is a feature that allows users to specify a traffic class independently of QoS policies.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00

QUESTION 32
On a Cisco switch, CDP v2 must be enabled for which AutoQoS configuration to function properly?

A. WTT queuing
B. trust boundary
C. fr-atm
D. ciscosoflphone

Answer: B

QUESTION 33
What three actions can reduce packet sizes on WAN links supporting converged VoIP and data? (Choose three)

A. Configure LFI to an average packet size for all traffic on the WAN link
B. Configure compressed RTP headers
C. Configure software payload compression

D. Configure hardware payload compression
E. Configure LFI to the same size as the voice packets.

Answer: B, C, E

QUESTION 34
What will happen when class-based header compression is configured without specifying RTP or TCP?

A. Only TCP headers will be compressed
B. Only RTP headers will be compressed
C. The unrecognized command warning is returned.
D. RTP and TCP headers will be compressed

Answer: D
CiscoPress QOS Study Guide page 474

QUESTION 35
What are the benefits, as listed in the DQOS course, for Enterprise Networks when QoS is implemented? (Choose all that apply.)

A. It sets traffic priorities across the network.
B. It allows better LAN performance through Per QOS Spanning Tree (PQST).
C. It minimizes loss during bursty congestion.
D. It allows for the disconnection of calls.
E. It reduces the amount of data sent through the network using Content Distribution Networking (CDN).

Answer: A, C

Explanation:
QoS attempts to solve network traffic performance issues, although QoS is not a cure-all.
To improve network performance, QoS features affect a network by manipulating the following network characteristics:
1) Bandwidth
2) Delay
3) Jitter (delay variation)
4) Packet loss
By the means of priorities QoS minimizes delay of packets.
Reference: Cisco Press - DQOS Exam certification Guide p.8

QUESTION 36
In which way does the Integrated Services model differ from the Differentiated Services model?

A. Integrated Services is more scalable than Differentiated Services.

B. Integrated Services provides traffic preferences, but no guaranteed delivery.
C. Integrated Services uses RSVP to signal the requested level of service, whereas Differentiated Services does not use any signaling.
D. Integrated Services does not make use of any signals whereas Differentiated Services uses signals to request level of services.
E. Integrated Services uses IP Precedence whereas Differentiated Services uses the DSCP.

Answer: C

Explanation:
Integrated Services model is introduced to supplement the best-effort delivery by setting aside some bandwidth for applications that require bandwidth and delay guarantees. The Integrated Services model expects applications to signal their requirements to the network. Resource Reservation Protocol (RSVP) is used to signal QoS requirements to the network.
Differentiated Services model is added to provide more scalability in providing QoS to IP packets. The main difference is that the network recognizes packets (no signalin is needed) and provides the appropriate services to them.
Reference: Introduction to IP QoS p.18

QUESTION 37
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know what are the best practices when designing a network for QoS. What will your reply be? (Choose all that apply.)

A. To color close to the application
B. To perform marking at WAN edge routers prior to packets exiting a WAN port.
C. To create a trust boundary as close as possible to the network edge.
D. To reclassify QoS settings near to the edge when devices seem dodgy and untrustworthy.
E. All of the above.

Answer: A, C, D

QUESTION 38
A CE to PE Frame Relay link is supporting VoIP and data traffic. When managed CE services are being used, which QoS mechanisms should typically be configured? (Choose four)

A. Frame Relay Traffic Shping (FRTS) on both the CE and PE
B. FRF 12 on both the CE and PE
C. WRED for all traffic classes on both the CE and PW
D. LLW on the CE and PE
E. class-based policing on the CE ingress for traffic to the customer
F. class-based policing ono the PE ingress for traffic to the customer

Answer: A, B, E, F

QUESTION 39
How does CB-Shaping adapt the shaping rate when BECNs are received?

A. The shape-adaptive min-rate command adapts the shaping rate when FECN bits are received
B. Each BECN bit causes the shaping rate to be reduced by three-quarters of the previous rate, but not below the min-rate
C. When FECN bits are received, it causes the transmit shaping rate to be reduced by one-half, but not below the min-rate
D. The shaping rate will increase slowly once there have been 16 intervals of no FECNs.

Answer: B
Page 338, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 40
Which term describes the amount of time it takes to place all of the bits in a packet onto a wire?

A. queuing delay
B. processing delay
C. propagation delay
D. serialization delay
E. prioritization delay
F. optimization delay

Answer: D
Page 15, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 41
How is AutoQoS related to MQC?

A. AutoQoS implements classes and policies defined earlier in MQC
B. duplicates policies defined in MQC from one device to another
C. generates MQC classes and policy map templates
D. runs an interactive script to guide the administrator through MQC

Answer: C
Page 2, Cisco AutoQoS White Paper,
http//www.cisco.com/en/US/tech/ CK5 43/ CK7 59/technologies_white_paper09186a00801348bc.shtml

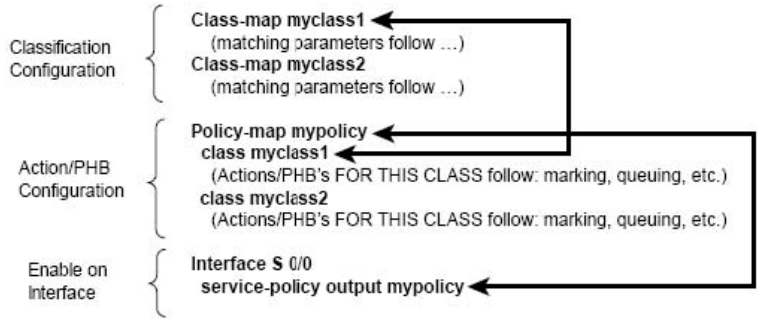
---

QUESTION 42
The newly appointed Certkiller trainee technician wants to know what steps are used to implement QoS using Modular QoS Command Line Interface (MQC). What will your reply be? (Choose all that apply.)

A. Select an output queuing strategy using a queue map.
B. Attach the QoS traffic policy to an interface in the inbound or outbound direction.
C. Configure marking options using a route map.
D. Configure classification options using a class map.
E. Configure a QoS traffic policy by associating a QoS traffic class with a QoS feature.

Answer: B, D, E

Explanation:
Figure 3-9 *MQC Commands and Their Correlation*



Implementing QoS by using the MQC consists of three steps:
Step 1 Configuring classification by using the class-map command
Step 2 Configuring traffic policy by associating the traffic class with one or more QOS features using the policy-map command
Step 3 Attaching the traffic policy to inbound or outbound traffic on interfaces,
Sources: Cisco DQOS Exam Certification Guide, Pages 176, 177
Cisco IP QoS-Modular QoS CLI Classification, Page 8-5

QUESTION 43
What happens to traffic that does not have a match when using a Modular QoS Command Line Interface (MQC)?

A. It is ignored by the MQC
B. It is dropped (implicit deny all)
C. It is placed in the default class
D. It is process switched through the router

Answer: C

Explanation:
Modular Quality of Service Command-Line Interface (MQC)
The MQC is a command-line interface (CLI) structure that allows you to create traffic policies and attach

these policies to interfaces.
In the MQC, the class-map command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.
The Modular quality of service (QoS) CLI structure consists of the following three processes:
* Defining a traffic class with the class-map command.
* Creating a traffic policy by associating the traffic class with one or more QoS features (using the policy-map command).
* Attaching the traffic policy to the interface with the service-policy command.
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; that is, if you enter the class-map cisco command while configuring the traffic class in the CLI, the traffic class would be named "cisco".
The 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.
Source:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bcd.html

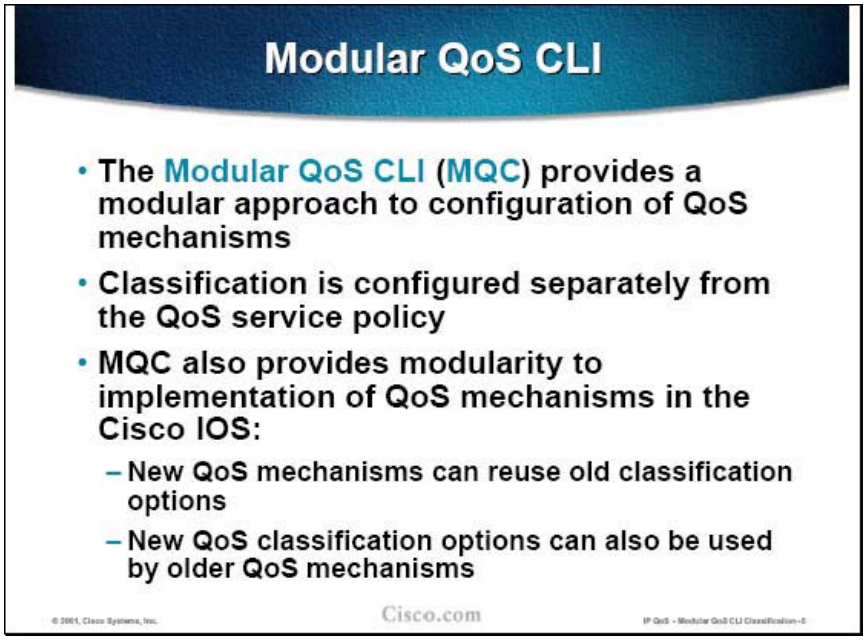
---

QUESTION 44
What functions do policies fulfill in the Modular QoS Command Line Interface (MQC)?

A. It is used to bind policies to the interfaces.
B. It is used to define the policies for classifying data.
C. It is used to bind traffic classifications to QoS policies.
D. It is used to apply end-to-end policies in network devices.

Answer: C

Explanation:



The Quality of Service mechanisms that have been added to the Cisco IOS all had their own set of classification options. For example:
1472;Committed Access Rate (CAR) can classify packets by using:
- Access lists
- QoS group
- DSCP
- Rate limit access list

61472;Traffic Shaping (GTS) can classify packets by using access lists
61550;Priority Queuing (PQ) and Custom Queuing (CQ) can classify packets by using:
- Access lists
- Packets size
- Fragment
- TCP or UDP port number

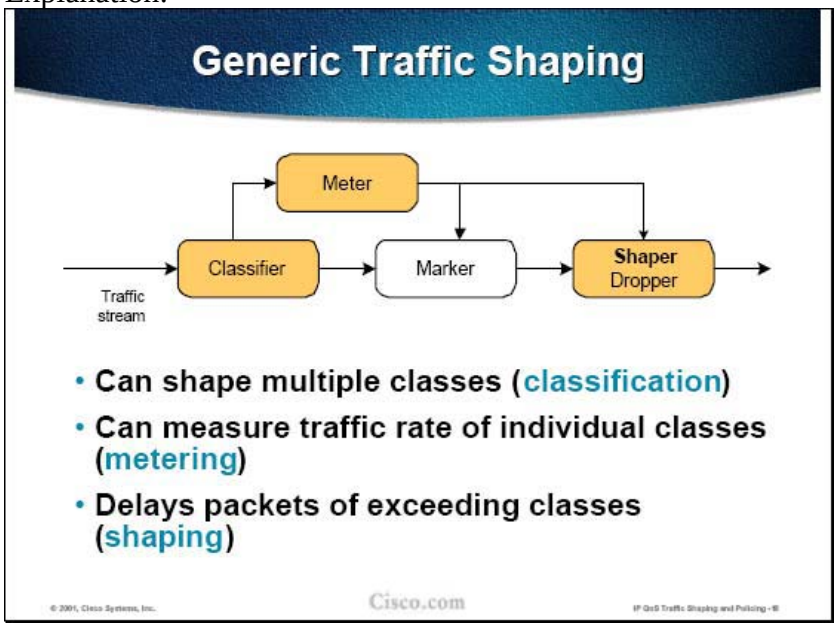
The Modular Quality of Service Command Line Interface (MQC) was introduced to allow any supported classification to be used with any QoS mechanism.
The separation of classification from the QoS mechanism allows new IOS versions to introduce new QoS mechanisms and reuse all available classification options. On the other hand, old QoS mechanisms can benefit from new classification options.
Another important benefit of the MQC is the reusability of configuration. MQC allows the same QoS policy to be applied to multiple interfaces. CAR, for example, required entire configurations to be copy-pasted between interfaces and modifying configurations was tiresome.
The Modular QoS CLI, therefore, is a consolidation of all the QoS mechanisms that have so far only been available as standalone mechanisms.
This module focuses on the classification element of the Modular QoS CLI.
Source: Cisco IP QoS-Modular QoS CLI Classification, Pages 8-3, 8-4

QUESTION 45
How is congestion managed through the use of Generic Traffic Shaping (GTS)?

A. Strict priority is maintained for classified traffic and is policed through packet discard.
B. Random Early Detection is used to selectively drop packets and avoid congestion.
C. Outbound traffic is constrained to a particular bit rate using a token bucket mechanism.
D. Call Admission Control is performed on classified traffic to ensure allocated bandwidth is not exceeded.
E. Using multiple traffic queues that are services in a round robin fashion promotes fairness and reduces congestion.

Answer: C

Explanation:



Generic Traffic Shaping (GTS) shapes traffic by reducing the outbound traffic flow
to avoid congestion. This is achieved by constraining traffic to a particular bit rate using the token bucket mechanism. GTS is applied on a per-interface basis and can
use access lists to select the traffic to shape. It works with a variety of Layer-2 technologies, including Frame Relay, ATM, Switched Multi-megabit Data Service (SMDS) and Ethernet.
As shown in the block diagram, GTS performs three basic functions:
n Classification of traffic, so that different traffic classes can have different policies applied to them
n Metering, using a token-bucket mechanism, to distinguish between conforming and exceeding traffic
n Shaping, using buffering, to delay exceeding traffic and shape it to the

configured rate limit
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-15

QUESTION 46
Exhibit:
interface Hssi0/0/0
description 45Mbps to R2
rate-limit output access-group 101 20000000 24000 32000
conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0
rate-limit output access-group 102 10000000 24000 32000
conform-action set-prec-transmit 5
exceed-action drop
rate-limit output 8000000 16000 24000
conform-action set-prec-transmit 5 exceed-action drop
ip address 10.1.0.9 255.255.255.0
!
access-list 101 permit tcp any any eq www
access-list 102 permit tcp any any eq ftp
What happens to WWW traffic sent out to the HSSI interface?

A. WWW traffic rate limited to 80 MB.
Traffic exceeding the rate policy is dropped.
B. WWW traffic is limited to 10 MB.
Conforming traffic is sent as IP Precedence 5.
Traffic exceeding the rate policy is dropped.
C. WWW traffic is limited to 20 MB.
Conforming traffic is sent as IP Precedence 5.
Traffic exceeding the rate policy is sent with best effort priority,
D. WWW traffic is limited to 20 MB.
Conforming traffic is marked as IP Precedence 5 and the next rare limit statement is executed.
Traffic exceeding the rate policy is sent with best effort priority.

Answer: C

QUESTION 47
When configuring Frame Relay Traffic Shaping (FRTS) on Cisco routers, how are traffic rates and shaping parameters defined?

A. FRTS parameters are configured using a policy map.
B. A Frame Relay map class is used to define these parameters.
C. These parameters are configured on the Frame Relay interface.
D. All FRTS parameters should be configured using the Modular QoS Command Line Interface (MQC).
E. The traffic rate is defined on the interface and the remaining QoS parameters are

defined using either a QoS Group or a policy map.

Answer: B

Explanation:
Enabling FRTS on an interface enables both traffic shaping and per-VC queuing on all the interface's PVCs and SVCs. Traffic shaping enables the router to control the circuit's output rate and, if configured, to react to conjection notification information. Queuing enables per-VC scheduling of traffic to be shaped.
Configuring FRTS involves:
1) Defining the shaping parameters with the map-class command
2) Enabling FRTS on the physical interface
3) Applying the shaping parameters to all, or selected, VCs on that interface.
Reference: Introduction to IP QoS (course) p.4-48

QUESTION 48
router(config-pcmap-c)#random-detect dscp-based
router(config-pcmap-c)#random-detect dscp af31 10 20 30
Given the router config, which two are true?

A. when the average queue size reaches 30 packets in depth, 1 out of 10 packets will be dropped
B. when the average queue size > 30, all packets will be tail-dropped
C. WRED will not drop any packets until the average queue length reaches 10
D. when the average queue size reached the max threshold, one out of every 30 packets will be dropped
E. All DSCP AF3x classes will use this profile unless otherwise specified

Answer: C, D
Page 443, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 49
Command exhibit: mis qos trust pass-through dscp
Your apprentice Certkiller is configuring a Catalyst 2950 Switch. What is the purpose of the command she is submitting (see exhibit)?

A. The command configures a port to trust the incoming CoS and not modify the incoming DSCP when sending the frame out.
B. The command configures a port to trust the incoming CoS and to generate the internal DSCP based on the incoming CoS. The internalr DSCP will then determine the gress DSCP.
C. The command configures a port to trust the incoming CoS and DSCP values.
D. The command configures a port to trust the incoming CoS and to generate the internal DSCP based on the incoming DSCP. The internal DSCP will then determine the egress DSCP.

E. The command configures a port to trust the incoming CoS and bypass the CoS-to-DSCP maps for generating the internal DSCP.
F. The command configures a port to trust the incoming CoS and bypass the DSCP-to-CoS maps for generating the egress CoS.

Answer: A

Explanation:
When the switch is in pass-through mode, it uses the CoS value of incoming packets without modifying the DSCP value and sends the packets from one of the four egress queues. By default, pass-through mode is disabled. The switch assigns a CoS value of 0 to all incoming packets without modifying the packets. The switch offers best-effort service to each packet regardless of the packet contents or size an dends it from a single egress queue.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps5213/products_configuration_guide_chapter09186a0

QUESTION 50
What are three benefits of using MQC for QoS configuration?

A. It allows the same QoS policy to be applied to multiple interfaces.
B. It provides support for up to 64 different class maps.
C. It allows any supported classification mechanism to be used with any QoS mechanism.
D. It allow for extensive marking capabilities to be applied to any service policy.
E. Classification is configured independently from the service policy.

Answer: A, C, E

Explanation:
The Modular Quality of Service Command Line Interface (MQC) was introduced to allow any supported classification to be used with any QoS mechanism.
The separation of classification from the QoS mechanism allows new IOS versions to introduce new QoS mechanisms and reuse all available classification options. On the other hand, old QoS mechanisms can benefit from new classification options.
Another important benefit of the MQC is the reusability of configuration. MQC allows the same QoS policy to be applied to multiple interfaces.
Reference: Introduction to IP QoS p.8-3

QUESTION 51
Which 3 options may be used on Cisco Catalyst switches for classifying IP Packets? (Choose 3)

A. 802.1Q
B. ISL CoS
C. Priority
D. MED

E. 802.1E

Answer: A, B, C

QUESTION 52
Which three QoS markers can be set using class-based marking? (Choose three.)

A. discard-threshold
B. qos-group
C. mpls exp bits
D. cos
E. becn
F. fecn

Answer: B, C, D

Explanation:
Class-based Marking supports following markers:
1) IP precedence
2) DSCP
3) QoS group
4) MPLS expertimental bits
5) ATM CLP bit
6) Frame Relay DE bit
7) 802.1Q/ISL cos/priority
Reference: IP QoS Introduction p.64

QUESTION 53
Based on Cisco's best practice recommendation, where should classification and marking be applied in a network?

A. in the core
B. at the access layer
C. at the distribution layer
D. as close to the source as possible
E. as close to the desalination as possible

Answer: D

Explanation:
Good QoS design calls for the marking of packets close to the source of the packet.
Reference: DQOS Exam Certification Guide p.849

QUESTION 54
You work as a network administrator at Certkiller .com. You are required to implement prioritizing, protection, and isolation of traffic based on marking.

Which mechanism should you deploy?

A. classification and marking
B. congestion management
C. congestion avoidance
D. metering
E. policing
F. shaping

Answer: B

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

QUESTION 55
When RED is used as a dropping mechanism to avoid a full queue, which problem is exhibited if the minimum threshold and the maximum threshold are too close in size?

A. Queues fill and tail-drop drops packets.
B. The mark probability denominator is set to zero.
C. The default average queue size is rest to 512 packets.
D. TCP global synchronization can occur.

Answer: D

Explanation:
When congestion occurs, dropping affect most of the TCP sessions, which simultaneously back-off and then restart again. This causes inefficient link utilization at the congestion point (TCP global synchronization).
Reference: Introduction to IP QoS p.5-4

QUESTION 56
Which Cisco IOS feature must be enabled before configuring class-based marking?

A. FEC
B. netflow
C. CEF
D. QBBP
E. Tcp small-server
F. ip classless

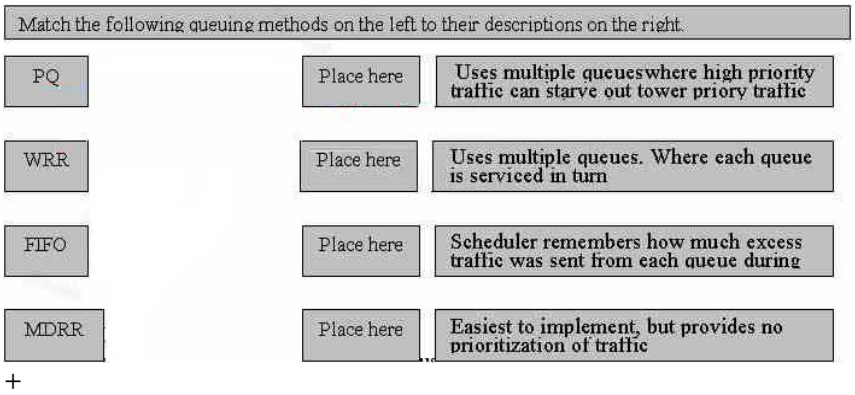
Answer: C

QUESTION 57
When queue on the Catalyst 2950 can be configured as the expedite queue?

A. queue 1
B. queue 2
C. queue 3
D. queue 4

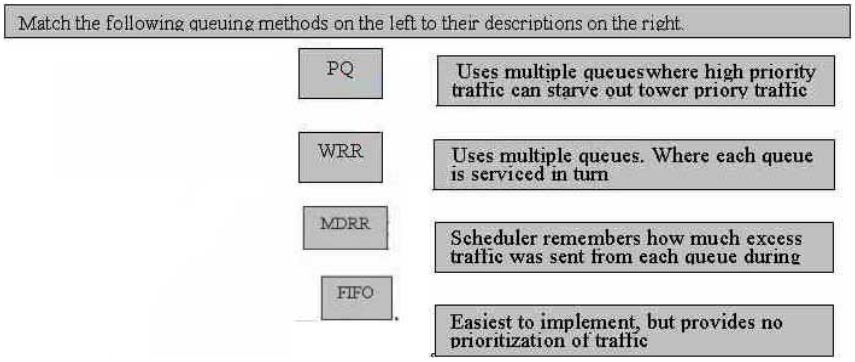
Answer: D

QUESTION 58
DRAG DROP



+

Answer:



QUESTION 59
Which three prerequisites must be met before using AutoQoS? (Choose three.)

A. Cisco Express forwarding (CEF) must be enabled at the interface or ATM PVC.
B. Preconfigured policy maps must exist for AutoQoS to operate correctly.
C. AutoQoS cannot be configured if a service policy is attached to an interface.
D. The no ip address command is required for all interfaces or subinterfaces with link speeds less than 768 kbps.
E. On all interfaces or subinterfaces, the correct bandwidth should be configured with the bandwidth command.

Answer: A, C, E

QUESTION 60
What are the three primary challenges when dealing with a converged network that QoS can help solve? (Choose three.)

A. delay
B. packet loss
C. server congestion
D. lack of bandwidth
E. port overutilization

Answer: A, B, D

Explanation:
QoS can solve following issues:
1) Lack of bandwidth - multiple flows are contesting for a limited amount of bandwidth
2) Too much delay - packets have to traverse many network devices and links that add up to the overall delay
3) Variable delay - sometimes there is a lot of other traffic which results in more delay
4) Drops - packets have to be dropped when a link is congested

---

QUESTION 61
Configuration:
Policy-map shape-cbwfq
Class interactive
Shape average 256000
Shape adaptive 128000
Bandwidth 128
Based on the configuration, which two statements are true? (Choose two.)

A. The interactive traffic class will have a minimum bandwidth guarantee of 256 kbps.
B. The interactive traffic class will have a maximum bandwidth guarantee of 256 kbps.
C. If the interactive traffic class exceeds an average rate of 256 kbps. The traffic rate will be throttled down to 128 kbps.
D. This configuration allows class-based traffic shaping to lower the traffic rate in response to the BECN bit.
E. The interactive traffic class will have a min-rate (min-cir) of 128 kbps.

Answer: C, E

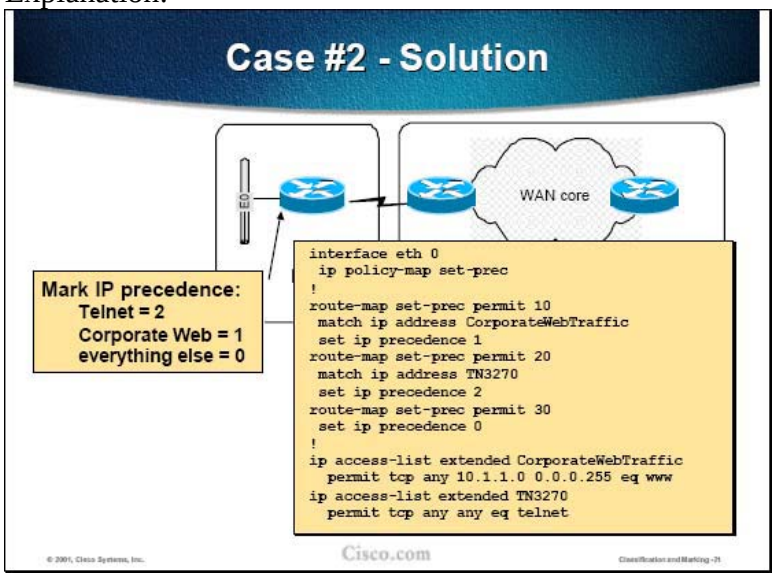
QUESTION 62
Given the router configuration:
interface Ethernet 0
ip address 10.1.1.1 255.255.255.0

ip policy-map set-prec
!
route-map set-prec permit 10
match ip address 101
set ip precedence 1
!
route-map set-prec permit 20
set ip precedence 0
!
access-list 101 permit tcp any any eq telnet
!
According the configuration illustrated above which of the following statements is valid?

A. All telnet packets from the Ethernet 0 interface are marked with IP precedence 0.
B. All packets sourced locally by the router that goes out on the Ethernet 0 interface are marked with IP precedence 1.
C. All non-telnet traffic from the Ethernet 0 interface is marked with IP precedence 0.
D. All telnet packets sourced locally by the router that goes out on the Ethernet 0 interface are marked with IP precedence 1.

Answer: C

Explanation:



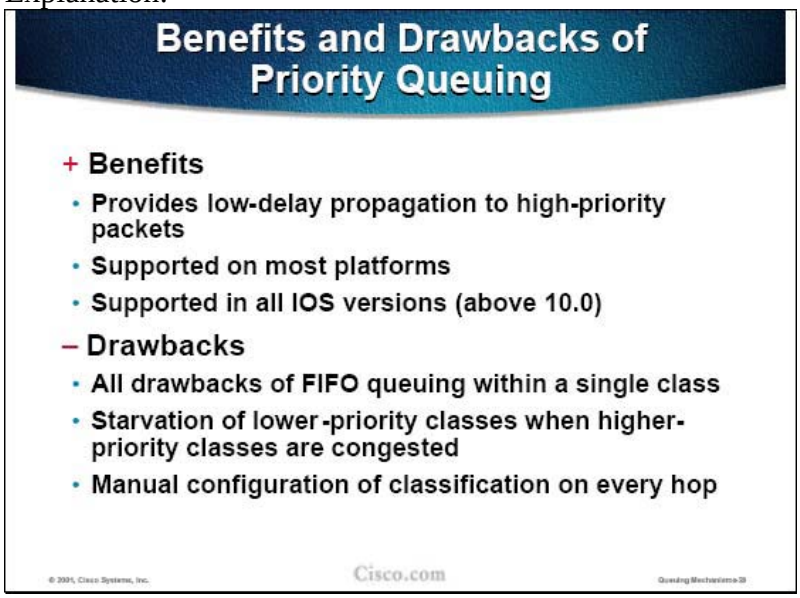
A route map is created with three statements, one for each application:
The first statement uses an access list to identify corporate web traffic (destination port 80). IP precedence 1 is applied to these packets.
The second statement uses another access list to identify outbound telnet sessions. IP precedence 2 is applied to these packets.
The last statement sets IP precedence 0 to all other packets.
Source: Cisco IP QoS Classification and Marking, Page 2-19

QUESTION 63
What is the result of properly configured Priority Queuing on Cisco IOS routers?

A. A starvation condition can occur where lower priority queues are never serviced.
B. Priority Queuing overhead can be too taxing on slow WAN links and might result in buffer exhaustion.
C. By default, unclassified packets are placed into the high priority output queue, which can affect high priority traffic.
D. The high priority queue has a default queue limit of 80, that can result in excessive packet loss.

Answer: A
Incorrect:
C. By default, unclassified packets are placed into the normal priority output queue.
D. The high priority queue has a default queue limit of 20.

Explanation:



As mentioned previously, Priority Queuing suffers from the same drawbacks as FIFO queuing, except it is localized to four classes. Each class can experience starvation, delay and jitter if one or more flows in the class cause congestion.
Furthermore, one higher-priority queue can cause all other queues to starve if it is congested.
Priority Queuing requires manual configuration of classification.
The main benefit of PQ is that it enables the user to create a class that is used for applications that require low delay (high queue).
Source: Cisco Queuing Mechanisms, Page 3-24

QUESTION 64
What is the default match strategy for a class map?

A. match none
B. match any
C. match some
D. match all
E. match one

Answer: D

Explanation:
There are two ways of processing conditions when there is more than one condition in a class map:
1) Match all - all conditions have to be met to bind a packet to the class
2) 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".
Reference: Introduction to IP QoS p.8-6

QUESTION 65
Which one of the following configurations provides a maximum bandwidth guarantee of 192 kbps for the real-time traffic class?

A. class real-time
bandwidth 192
B. class real-time
Priority 192
C. class real-time
Shape peak 192000
D. class real-time
Shape average 192000
E. class real-time
police 192000 conform-action transmit exceed-action drop

Answer: B

Explanation:
For real-time traffic class maximum bandwidth guarantee is configured using priority command.

QUESTION 66
The Tx Ring always uses which queuing method?

A. PQ
B. CQ
C. DRR
D. FIFO
E. WFQ
F. CBWFQ

Answer: D

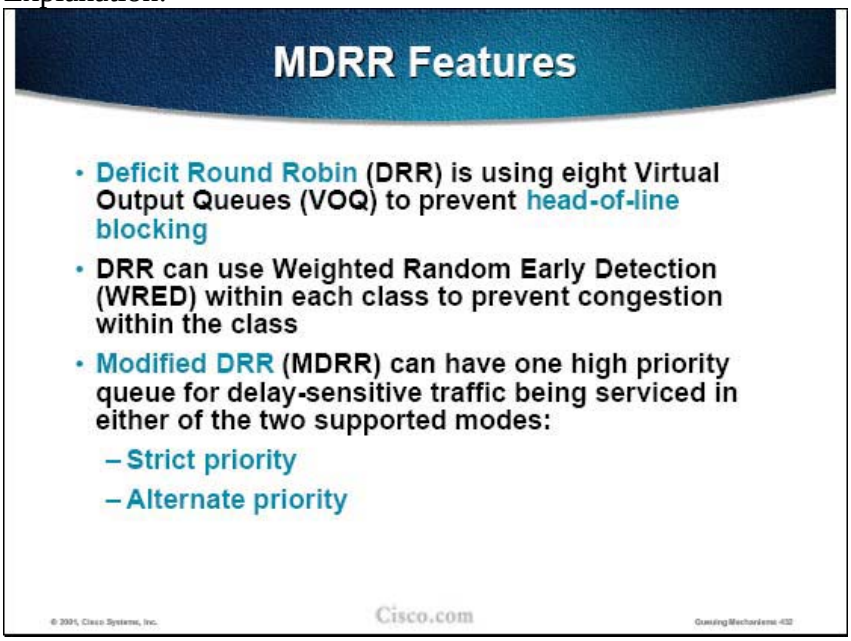
Explanation:
The following list summarizes the key points about TX Rings and TX Queues in relation to their effect on queuing:
1) The TX Queue/TX Ring always performs FIFO scheduling, and cannot be changed.
2) The TX Queue/TX Ring uses a single queue, per interface.
3) IOS shortens the interface TX Queue/TX Ring automatically when an output queuing method is configured.
4) The TX Ring/TX queue length can be configured to a different value.
Reference: DQOS Exam Certification Guide p.245

QUESTION 67
Modified Deficit Round Robin (MDRR) service algorithm is capable of supporting which of the following operating modes? (Choose all that apply.)

A. FIFO
B. weighted priority
C. strict priority
D. shared priority
E. alternate priority

Answer: C, E

Explanation:



DRR was the first implementation that was later improved by allowing one queue to be high priority.
Source: Cisco Queuing Mechanisms, Page 3-120

QUESTION 68
Which two procedures are required to configure AutoQoS on a Cisco router?
(choose two)

A. Enable CEF globally
B. Configure map-class for AF traffic
C. Configure service-class for voice
D. Set the clock rate on the interface
E. Set the bandwidth statement on the interface

Answer: A, E
Page 163, Cisco QOS Exam Certification Guide (IP Telephony Self-Study), 2nd Edition,
http//www.ciscopress.com/title/1587201240

QUESTION 69
Which command is used to configure DSCP-based CB-WRED on an interface?

A. weighted-random dscp-based
B. random-queue dscp
C. random-detect dscp-based
D. weighted-queue dscp

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

QUESTION 70
Within CBWFQ, what is the default dropping scheme used when a CBWFQ class queue reaches its configured queue limit?

A. WRR
B. tail drop
C. WRED
D. RED

Answer: B
Reference: Page 273, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 71
Which queuing method solves the problems created by inaccuate round-robin byte counting?

A. PQ
B. DRR

C. FIFO
D. MWRR

Answer: B

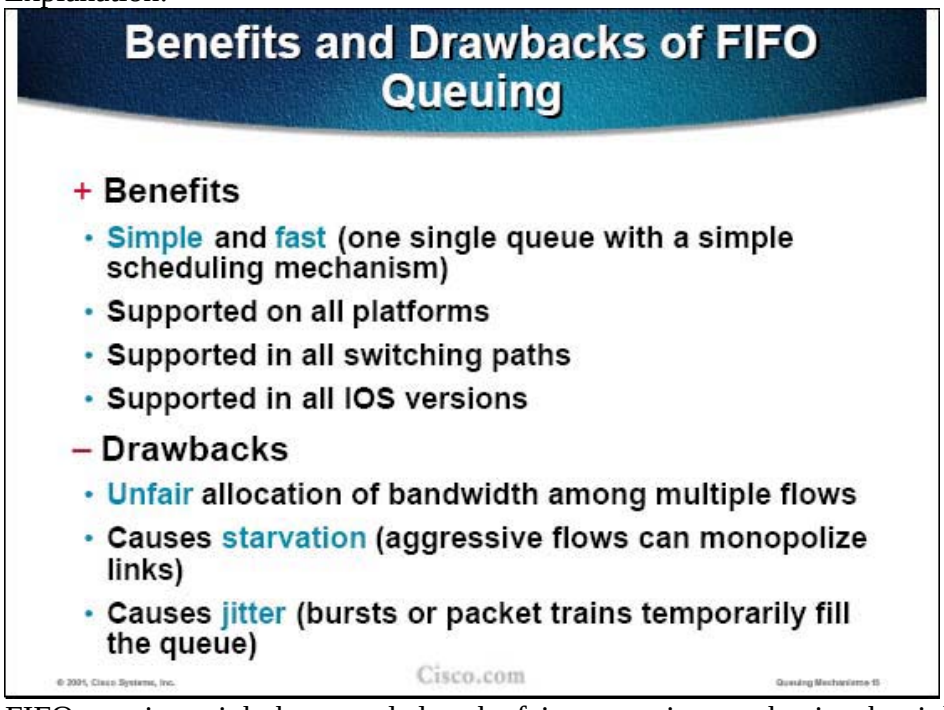
Explanation:
DRR can use Wighted Random Early Detection (WRED) within each class to prevent congestion within the class.
The scheduling of DRR is similar to that of Custom Queuing, except it is more accurate.
DRR remembers the number of bytes it sent above the threshold in the previous roung (deficit).
Reference: Introduction to IP QoS p.3-123

QUESTION 72
Which of the following statements represents a disadvantage of FIFO queuing?

A. FIFO queuing produces excessive jitter.
B. FIFO queuing supports packets of queue size of 40 exclusively.
C. FIFO queuing can only support packet classification based upon traffic flows.
D. FIFOI queuing is only available on interfaces that operate at 2 Mbps or higher.

Answer: A
Incorrect:
D: Disable WFQ to enable FIFO on interfaces that have less than 2Mbps of bandwidth

Explanation:



FIFO queuing might be regarded as the fairest queuing mechanism but it has a long list of drawbacks:

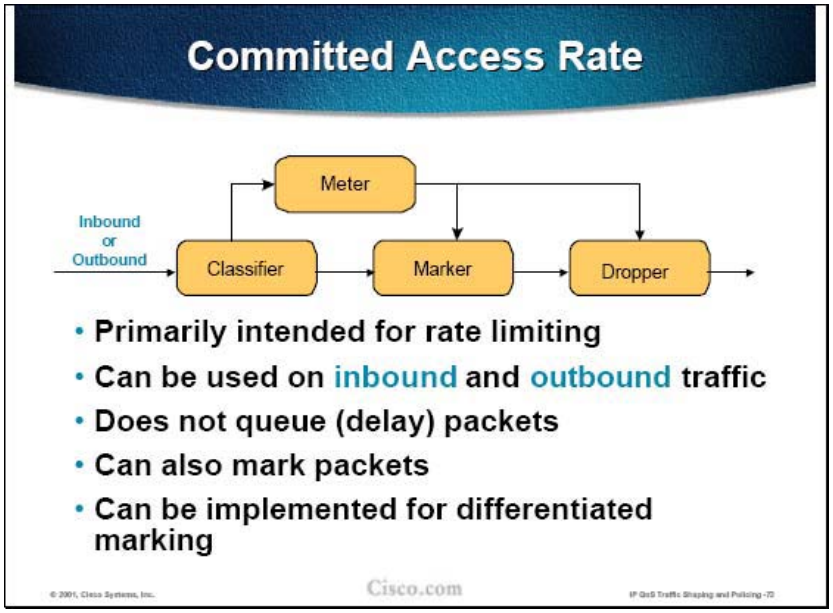
FIFO does not fairly allocate bandwidth among multiple flows. Some flows receive more bandwidth because they use larger packets or send more packets.
FIFO is extremely unfair when an aggressive flow is contesting with a fragile flow. Aggressive flows send a large number of packets, many of which are dropped. Fragile flows send a modest amount of packets and most of them are dropped because the queue is always full due to the aggressive flow. This type of behavior is called starvation.
Short or long bursts cause a FIFO queue to fill. Packets entering an almost full queue have to wait a long time before they can be transmitted. Another time, the queue might be empty causing packets of the same flow to experience almost no delay. Variation in delay is called jitter.
In spite of all the drawbacks FIFO is still the most used queuing mechanism because of the following benefits:
It is simple and fast. Most high-end routers with fast interfaces are not really challenged by the drawbacks mentioned earlier. Furthermore, routers are not capable of complex classification and scheduling when they have to process a large number of packets per second. FIFO is, therefore, the most suitable queuing mechanisms on these platforms.
It is supported on all platforms.
It is supported in all IOS versions.
Source: Cisco Queuing Mechanisms, Page 3-12

QUESTION 73
The newly appointed Certkiller trainee technician wants to know what services are provided through Committed Access Rate (CAR). What will your reply be? (Choose all that apply.)

A. Link efficiency
B. Traffic shaping
C. Policing
D. Classification
E. Weighted Random Early Discard (WRED)

Answer: C, D

Explanation:



Committed Access Rate (CAR) provides the capability to allow the service provider to rate-limit traffic in and out of router interfaces, thereby enabling various forms of ingress and egress rate-limiting in a network. CAR is a policing mechanism, not a queuing mechanism. Therefore it does not buffer or delay packets, which do or do not conform to the policy, but simply rate-limits them according to a simple "forward or drop" policy, according to the configuration. CAR also uses a token-bucket metering mechanism, similar to GTS, but without a delay queue.

The CAR rate-limiting feature manages a network's access bandwidth policy by ensuring that traffic falling within specified rate parameters is sent, while dropping packets that exceed the acceptable amount of traffic or sending them with a different priority. CAR is often configured on interfaces at the edge of a network to limit traffic into or out of the network.

CAR can also be used for packet marking. The operator can specify a policy that determines which packets should be assigned to which traffic class, and use CAR to implement the marking. The IP header already provides a mechanism to do this, namely the three precedence bits in the 'type of service' field in the IP header. CAR allows the setting of policies, based on information in the IP or TCP header such as IP address, application port, physical port or sub-interface, IP protocol, etc., to decide how the precedence bits should be marked or "colored." Once marked, appropriate treatment can be given in the backbone to ensure that premium packets receive premium service in terms of bandwidth allocation, delay control, etc.

Note CAR can also be used to police (or "recolor") precedence bits set externally to the network either by the customer or by a downstream service provider. Thus the network can decide to either accept or override external decisions.

CAR is implemented using the following abstract mechanisms:

61550;The classifier, which differentiates traffic into multiple classes, which may be treated in a discriminate manner

61472;The meter, which uses a token-bucket scheme to measure the rate of classified traffic

61472;The marker, which can be used to mark or re-mark classified traffic

(for example, with precedence or DSCP values)
61472;The dropper, which may drop packets (in the rate-limiting scenario)
according to the configured policy
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-68

QUESTION 74
Which of the following are shaping characteristics, but not policing characteristics?
(Choose all that apply.)

A. It forces TCP resends
B. It is rate limiting with no buffering mechanism
C. It can adapt to Frame Relay BECN and FECN
D. It is most typically performed on egress
E. None of the above.

Answer: C, D

QUESTION 75
Which of the following statements regarding the capabilities of CAR is valid?
(Choose all that apply.)

A. It is capable of supporting both policing and shaping options.
B. It allows a conform, exceed and violate action.
C. It allows cascading rate policies, in order to allow for more granular rate limits.
D. It can be used as both input and output policer.
E. It can be applied to serial interfaces, as well as ATM and Frame Relay interfaces.

Answer: C, D, E

QUESTION 76
Shaping is the process whereby traffic flow is examined and rates are measured.
What is done to packets during the shaping process when it exceeds a threshold bit
rate?

A. Packets are delayed (queued)
B. Packets are discarded
C. Packets that exceed a defined burst size as well, are delayed (queued)
D. Packets that exceed a defined burst size as well, are discarded

Answer: C
Traffic that exceeds the BC value in time interval T will be queued.
Ref
http://www.cisco.com/en/US/tech/ CK5 43/ CK5 45/technologies_tech_note09186a00800a3a25.shtml

---

QUESTION 77
Per-Virtual Circuit (VC) congestion avoidance discard at Layer 2 has what

consequence when the ingress ATM interface discards a fragment?

A. Incomplete data packets are sent and the entire data packet must be resent.
B. The entire data packet is discarded at the ingress interface and must be resent.
C. Incomplete data packets are sent and discarded packet fragments must be resent.
D. Data packets may be sent in cells that are out of order, causing the entire packet to be resent.

Answer: B, D

QUESTION 78
What are three capabilities of the route map used in policy-based routing? (Choose three)

A. Rate limiting
B. Packet marking
C. Packet classification
D. Intelligent packet discard
E. Defining customized routing paths

Answer: B, C, E

QUESTION 79
What are two services provided through Committed Access Rate (CAR)? (Choose two)

A. Policing
B. Classification
C. Link efficiency
D. Traffic shaping
E. Congestion avoidance

Answer: A, B

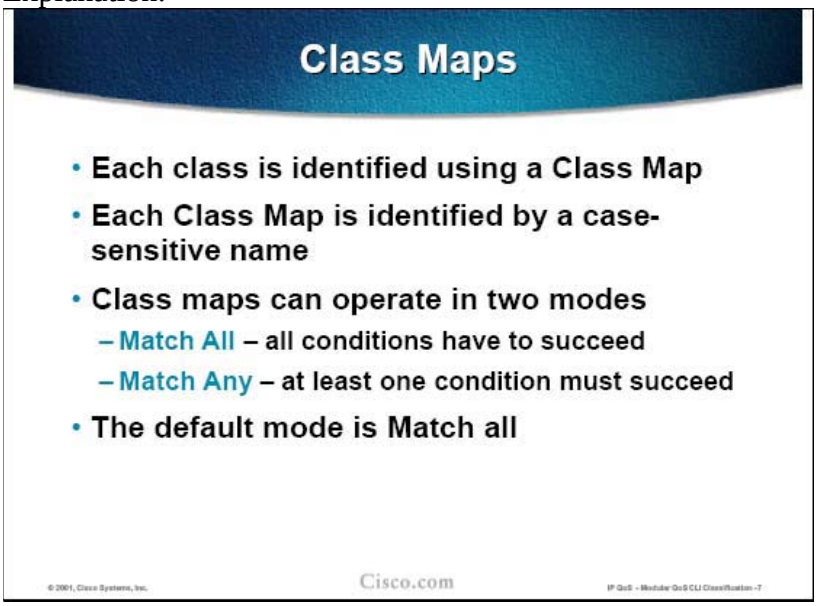
Explanation:
CAR provides policing functions and marking.
Policing, in its most basic form, discards traffic that exceeds a particular traffic contact. The contact has two components: a rate, stated either in bits per second or bytes per second; and a butst size, statted in either bits or bytes. The traffic conforms to the contract if it sends at the rate, or bellow, and it does not send a burst of traffic greater than the burst size. If the traffic exceeds the traffic rate over time, or exceeds the single burst size limit, the policing function drops the traffic in excess of the rate and the burst size. Therefore, the simplest form of policing has two rigid actions: eigher to forward packets or to drop them.
Reference: DQOS Exam Certification Guide p.194.

QUESTION 80
Which of the following statements regarding class maps is valid? (Choose all that apply.)

A. It is possible to configure a class map within another class map.
B. Match commands are used to specify packet classification.
C. The default behavior is match-any regardless whether match-any or match-all is specified or not.
D. Traffic that does not have a match in the class map is placed in the default class.

Answer: A, B, D
Incorrect:
C. The default mode is Match all.

Explanation:



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 if the packet belongs to the class.
There are two ways of processing conditions when there is more than one condition in a class map:
61472;Match all-all conditions have to be met to bind a packet to the class
61472;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".
Source: Cisco IP QoS-Modular QoS CLI Classification, Page 8-6

QUESTION 81
Study the Exhibit below carefully:
interface s0/0
custom-queue-list 5
!

queue-list 5 protocol ip 1 list 101
queue-list 5 queue 1 limit 40
queue-list 5 lowest-custom 2
queue-list 5 interface e0/0 2
queue-list 5 queue 2 byte-count 5000
queue-list 5 protocol ip 3
queue-list 5 queue 3 byte-count 5000
queue-list 5 queue 4 default
!
access-list 101 permit ip any any precedence 5
According to the configuration in the exhibit, which queue is used for traffic from e0/0 with a precedence of five?

A. 1
B. 2
C. 3
D. 4

Answer: A

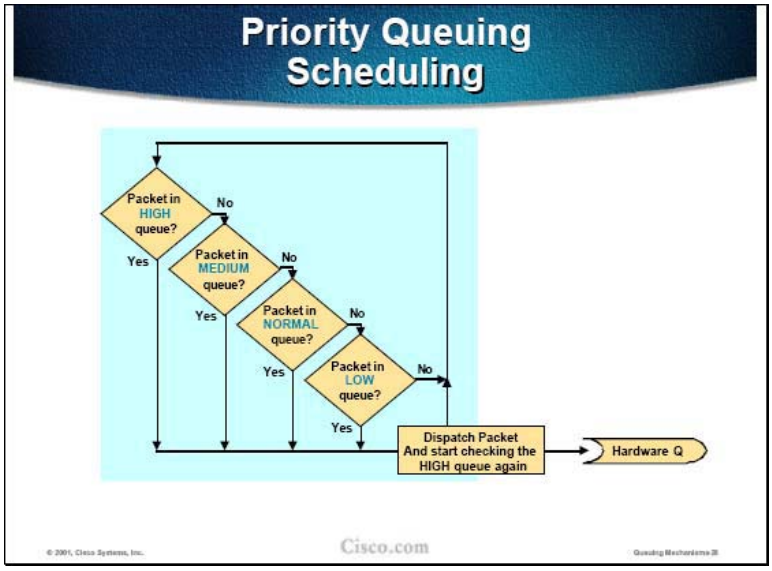
Explanation:
Answer should be A because the queue-List is processed top to bottom, so the Precedence 5 is meet before the interface ethernet 0/0.

QUESTION 82
Which of the following statements regarding the way in which Priority Queuing services its queues is valid?

A. The highest priority queue containing packets is serviced until it is empty.
B. The highest priority queue is always serviced first.
The remaining queues are serviced in a TDM fashion.
C. A high priority queue is serviced until it is empty, only then will the service engine move to the next highest priority queue in a round-robin fashion.
D. The highest priority queue is allocated 50% of the available bandwidth.
Each remaining queue is allocated half of the remaining bandwidth.

Answer: C

Explanation:



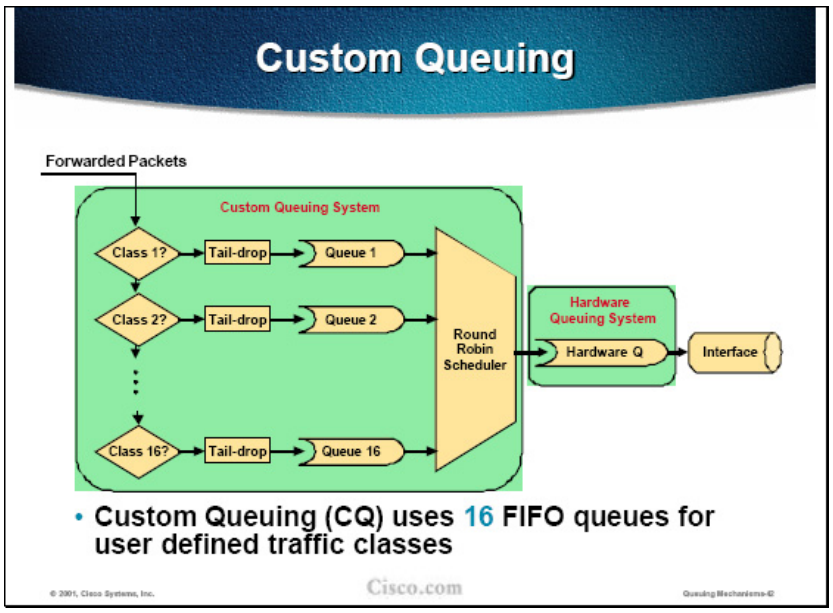
Priority Queuing uses strict priority scheduling. As long as there are packets in the high queue no other queue will be served. If the high queue is empty the router starts serving the medium queue.
Congestion in any of the queues, except the low queue, causes a different type of starvation. A congested higher-priority queue causes all lower-priority queues to starve (class starvation).
Source: Cisco Queuing Mechanisms, Page 3-23

QUESTION 83
What is the default scheduling mechanism that Custom Queuing uses?

A. FIFO
B. top down
C. round robin
D. weighted
E. none of the above

Answer: C

Explanation:



Custom Queuing (CQ) is similar to Priority Queuing in the way it is configured and in the supported classification options. The scheduling, however, is completely different. CQ uses up to 16 queues that can be used for user-defined classes. The classification options are identical to those of Priority Queuing.
The scheduling mechanism uses the round-robin service where each queue is allowed to forward a certain number of bytes (not packets).
Tail-drop is still used within each individual queue.
Source: Cisco Queuing Mechanisms, Page 3-35

QUESTION 84
Exhibit:
policy-map police 1
class bulk-ftp
police cir percent 20 pir percent 40
conform-action set-dscp-transmit af11
exceed-action set-dscp-transmit 0
violate-action drop
Based on the configuration, which two of the following statements are true? (choose two)

A. This configuration will use a single token buket
B. This configuration will drop all exceeding traffic
C. This is a dual-rate, class-based policing example
D. This is a percentage-based policing example
E. This is a multi-action, class-based policing example

Answer: C, D

Explanation:
The presence ofboth cir (Bc) and pir (Be)in the command make it a dual-rate policer. So

C is a valid answer.
The use of"percentage" makes D a valid answer.
Since all the "action" statements are on separate lines, it makes itmulti-action policing.
However, there is only one actual action being performed for each one. So E could be valid, and could not be valid.The question states to choose two answers.

QUESTION 85
What are three key differences between Weighted Fair Queuing (WFQ) and distributed Weighted Fair Queuing (dWFQ)? (Choose three)

A. dWFQ distributes its queuing policy to its neighbor.
B. dWFQ requires a Versatile interface Processor (VIP) to operate.
C. dWFQ adds WFQ support on ATM, Fast EtherChannel, and tunnel interfaces.
D. dWFQ supports classed-based weighting based on TOS field and QoS Group settings.
E. In order to use dWFQ, distributed Cisco Express Forwarding (dCEF) must be enabled on the interface.

Answer: B, D, E
Reference: Introduction to IP QoS p.4-18

QUESTION 86
When configuring Priority Queuing on Cisco IOS routers, which three steps are required? (Choose three)

A. Define the priority list.
B. Configure an ACL for traffic identification.
C. Assign packets to specific priority queues.
D. Specify the maximum size of the priority queues.
E. Assign the priority list to be a designated router interface.

Answer: A, C, E

Explanation:
The configuration of Priority Queuing can be split into the following four steps:
1. Classify data into four classes
2. Assign a queue to each class
3. Set the maximum queue size (if the default is not appropriate)
4. Apply the priority queuing system to one or more interfaces
Reference: Introduction to IP QoS p.3-25

QUESTION 87
What are two benefits of WFQ? (Choose two)

A. WFQ is very easy to configure, and no manual traffic classification is necessary
B. WFQ can provide fixed-bandwidth and fixed-delay guarantees
C. WFQ can provide fixed-bandwidth guarantees

D. WFQ can provide fixed-delay guarantees
E. WFQ prevents the large-volume flows with large packet size from staring out the low-volums flows with small packet size.
F. Based on DSCP, WFQ allows weighted, random dropping of packets when the WFQ system is full

Answer: A, E
The Question is WFQ and not CBWFQ, so the Answer should be: A,E

QUESTION 88
Which two statements are true about the DSCP field in an IP header? (Choose two)

A. DSCP is the most significant six bits of the DS field
B. DSCP is the least significant six bits of the DS field
C. DSCP is used to select the type of service (ToS)
D. DSCP is used to select a per-hop behaviour (PHB)
E. DSCP is broken into four sub0fields
F. DSCP is broker into five sub-fields

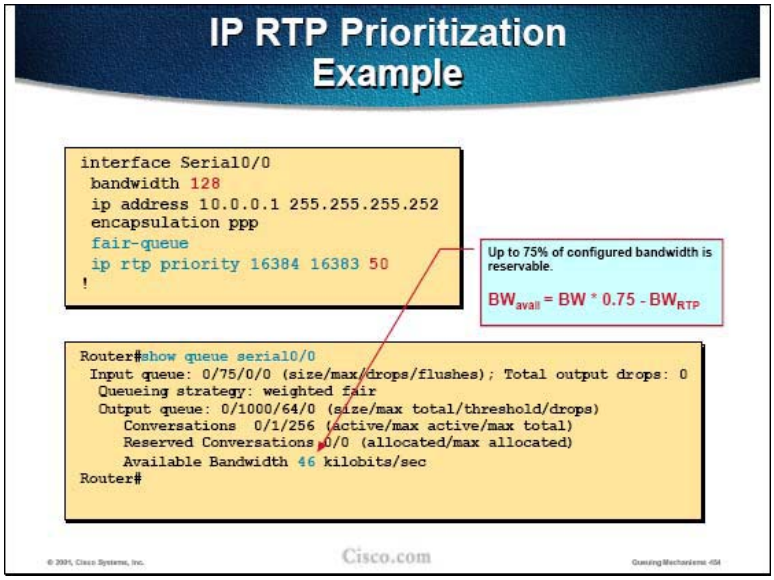
Answer: A, D
Page 120-121, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 89
Study the Exhibit below carefully:
interface s0/0
bandwidth 128
ip address 10.0.0.1 255.255.255.252
encapsulation ppp
fair-queue
ip rtp priority 16384 16383 50
According to the configuration in the exhibit, what is the amount of bandwidth available to the fair queues?

A. 46 Kbps
B. 50 Kbps
C. 65 Kbps
D. 78 Kbps
E. 128 Kbps

Answer: A

Explanation:



The sample configuration shows how 50 kbps of bandwidth is guaranteed for RTP traffic.
The show queue command shows there is only 46 kbps of bandwidth (128 kbps * 75% -50 kbps = 46 kbps) remaining for WFQ.
Source: Cisco Queuing Mechanisms, Page 3-140

QUESTION 90
Disregarding fragment size, which of the following LFI mechanism never fragments voice frames?

A. FRF .3
B. FRF.9
C. FRF.11 Annex C
D. FRF.6
E. FRF .12

Answer: C

Explanation:
FRF.11 Annex C never fragment voice frames.
Only this LFI mechanism is used with voice traffic.
There are three LFI mechanisms implemented in Cisco IOS:
1) Multilink PPP with Interleaving is by far the most common and widely used form of LFI.
2) FRF.11 Annex C LFI is used with Voice over Frame Relay (VoFR).
3) FRF.12 Frame Relay LFI is used with Frame Relay data connections.
4) In an ATM network, using separate PVCs carrying voice and data can be used to interleave packets when they are output on an interface.
Reference: Introduction to IP QoS p.6-47

QUESTION 91
Which of the following statements regarding cRTP compression is valid?

A. IP, TCP, and RTP headers are compressed, since the headers are uncompressed on the other end of the link.
B. UDP and RTP headers are compressed, but the IP header is not, so the VoIP packets can be delivered to the terminating gateway.
C. IP, UDP, and RTP headers are compressed, since the headers are uncompressed on the other end of the link.
D. TCP and RTP headers are actually removed, with a smaller header added that includes information that has changed since the last full header sent.
E. None of the above.

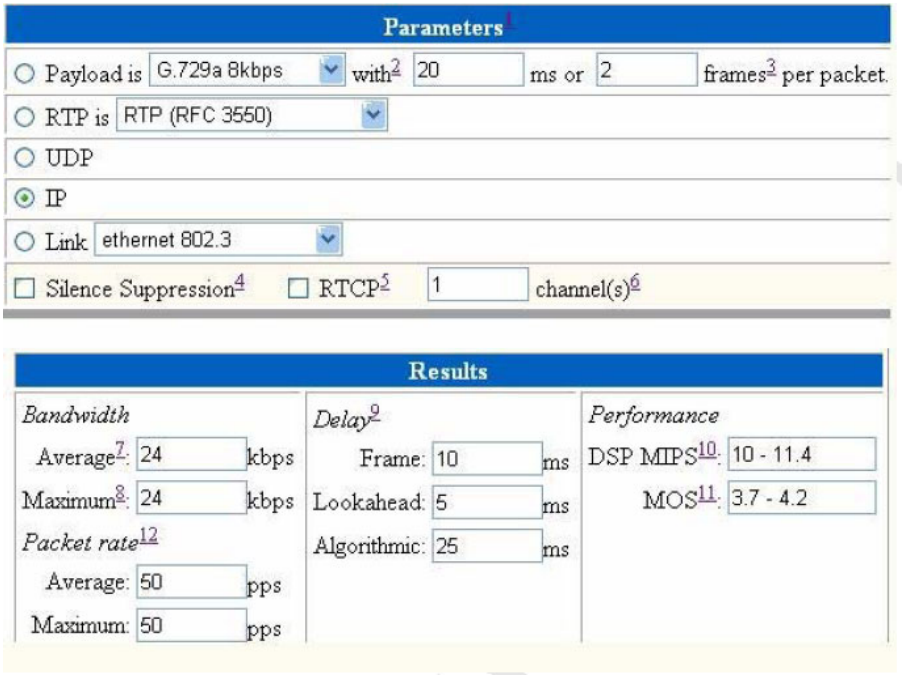
Answer: C

Explanation:
When using RTP compression IP packets that also have RTP headers are compressed. The compression algorithm does not compress the data-link header or trailer. It does compress the IP, UDP, and RTP headers. It does not compress any user data that follows the RTP header.

QUESTION 92
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know what the approximate bandwidths required for a G.729a VoIP call with and without cRTP enabled is. What will your reply be?

A. 5.3 Kbps/8 Kbps
B. 11 Kbps/26 Kbps
C. 12 Kbps/24 Kbps
D. 28 Kbps/64 Kbps
E. none of the above.

Answer: C

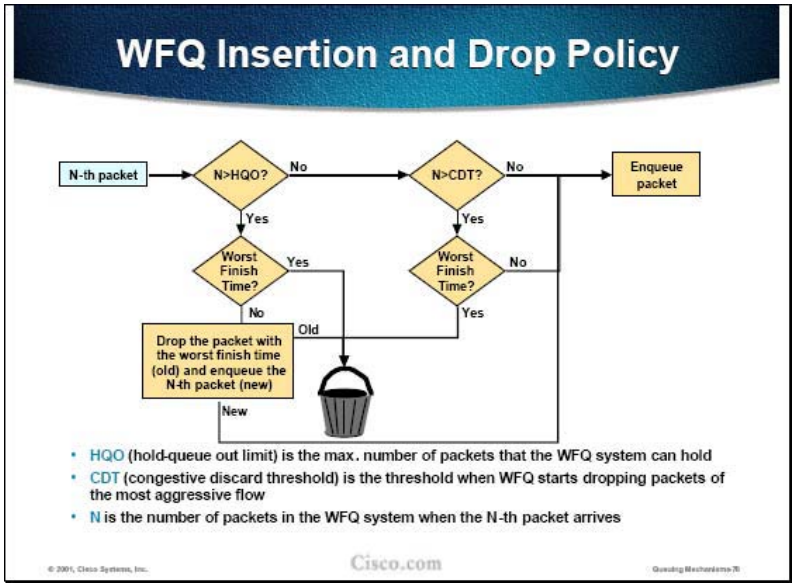


QUESTION 93
Which packet will most likely be dropped by Weighted Fair Queuing (WFQ) during periods of traffic congestion?

A. The newest packet.
B. The packet with the worst finish time.
C. The largest packet.
D. The packet with the lowest priority.

Answer: B

Explanation:



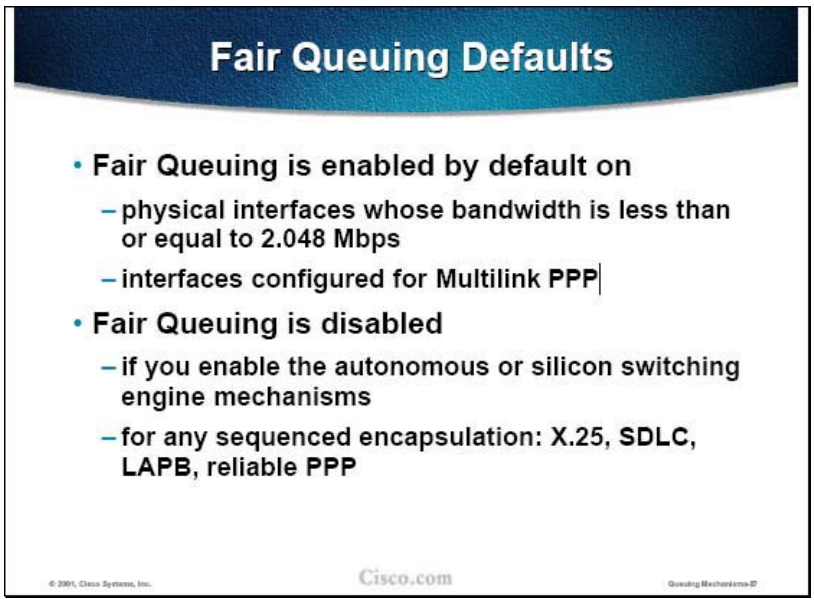
The figure illustrates the dropping scheme of WFQ. The process can be split into the following steps:
Step 1 Drop the new packet if the WFQ system is full (hold-queue limit reached) and the new packet has the worst finish time (the last in the entire system).
Step 2 Drop the packet with the worst finish time in the WFQ system if the system is full. Enqueue the new packet
Step 3 Drop the new packet if the queue, where the packet should be enqueued, is the longest (not in packets but in the finish time of the new packet) and there are more packets in the WFQ system than the CDT.
Step 4 Otherwise enqueue the new packet.
Source: Cisco Queuing Mechanisms, Page 3-61

QUESTION 94
The newly appointed Certkiller trainee technician wants to know what is the reason why Weighted Fair Queuing (WFQ) is disabled on WAN interfaces using X.25, SDLC, LAPB, or reliable PPP encapsulations. What will your reply be?

A. These protocols require strict priority scheduling which is not WFQ is not capable of supporting.
B. These encapsulations require sequenced packets which is contradictory to the way in which WFQ works.
C. Each of these protocols has a pre-defined compulsory queuing scheme.
D. These protocols require delay characteristics which WFQ-enabled routers are incapable of.

Answer: B

Explanation:



The figure explains the default behavior of WFQ. As mentioned previously, WFQ is automatically enabled on all interfaces slower than 2Mbps. WFQ is also required on interfaces using Multilink PPP.
WFQ cannot be used if reordering of frames is not allowed due to sequence numbering of Layer-2 frames or if the switching path does not support WFQ.
Source: Cisco Queuing Mechanisms, Page 3-79

QUESTION 95
Which of the following statements aptly describes what the result of enabling Weighted Fair Queuing (WFQ) on a low-speed router interface is?

A. Bandwidth is guaranteed for different traffic queues.
B. Delay is guaranteed for high-priority traffic types.
C. Fixed-size queues are pre-allocated for different traffic flows.
D. Low-bandwidth traffic receives priority over high-bandwidth traffic.

Answer: D

Explanation:
WFQ solves the problem of low-bandwidth traffic starvation. This is fair protocol and gives same bandwidth to all queues. For example if in queue 1 the packets are 100 kb each and in queues 2300kb each than 3 packets from queue 1 will go through the interface than 1 packet from queue 2 and so on.

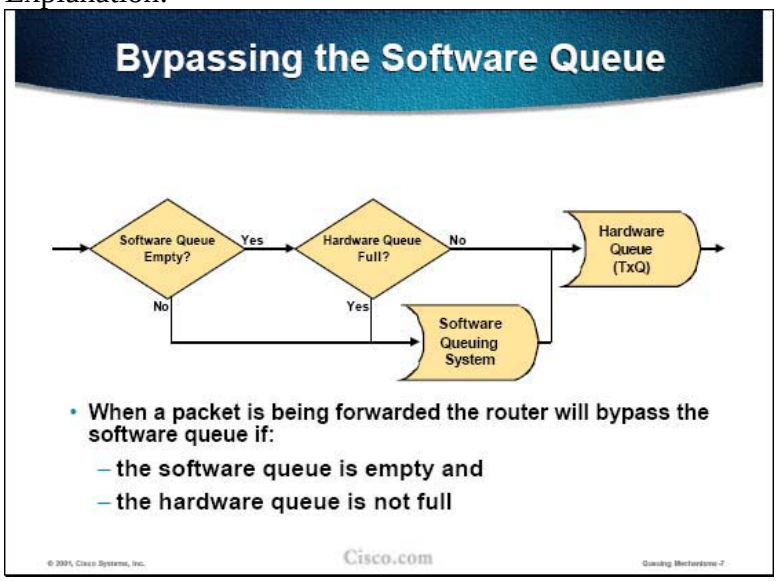
QUESTION 96
Under which circumstances will Cisco IOS bypass the transmit software queue on an interface and place the packet directly into the hardware queue?

A. When LLQ has been enabled.
B. When the software queue is full.

C. When the software queue is empty.
D. When the software queue has reached its MCC.

Answer: C

Explanation:



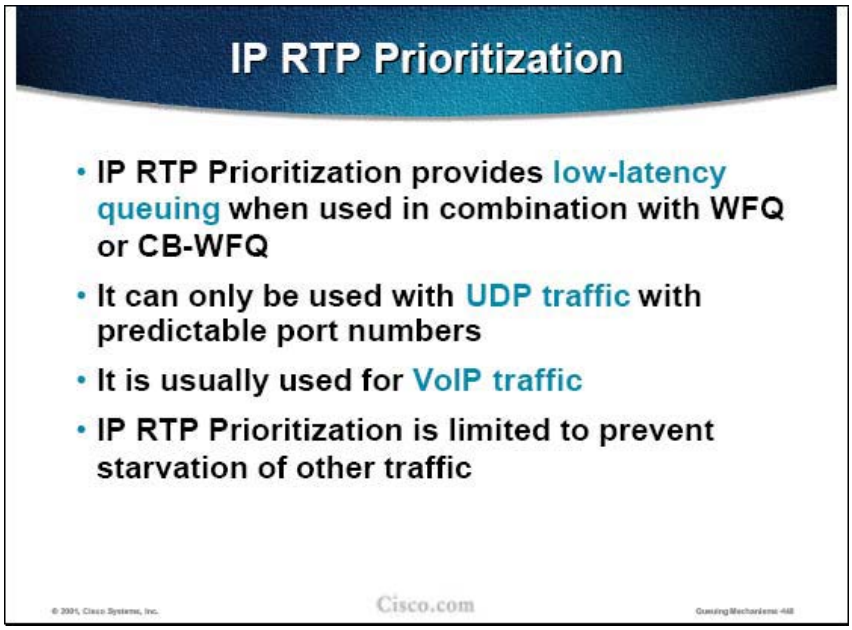
The implementation of software queuing was optimized for periods when the interface is not congested. The software queuing system is bypassed whenever there is no packet in the software queue and there is room in the hardware queue.
The software queue is, therefore, only used when data must wait to be placed into the hardware queue.
Source: Cisco Queuing Mechanisms, Page 3-6

QUESTION 97
Which of the following statements regarding the queuing scheme of IP Real Time Transport Protocol (RTP) prioritization is valid?

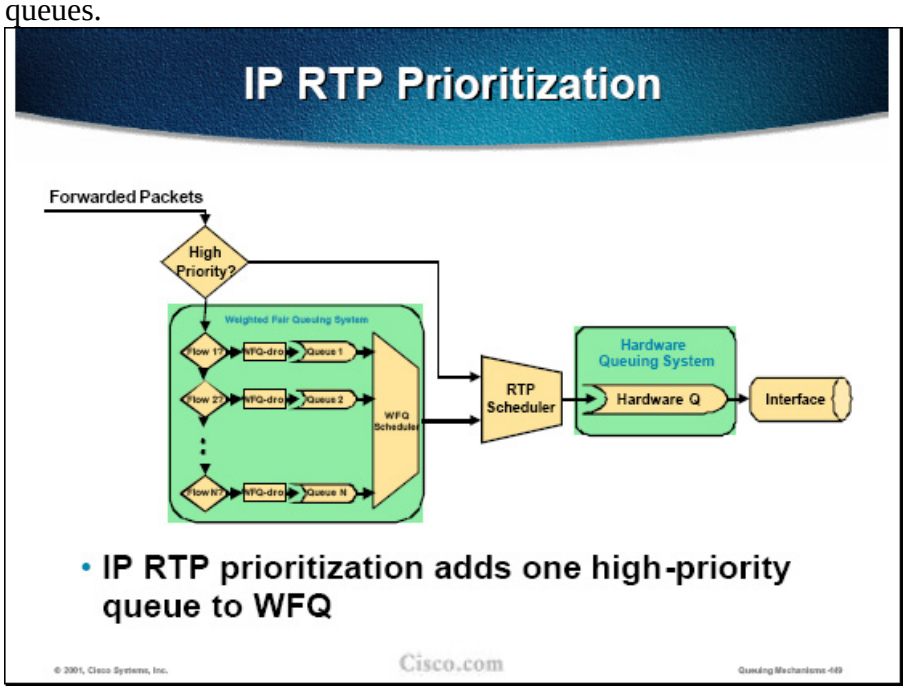
A. It is capable ofsupporting TCP traffic.
B. It is used mainly for interactive traffic.
C. It is responsible for providing low latency queuing by providing a high priority queue.
D. Packets that exceed the queue's configured rate are placed into the default queue.

Answer: C

Explanation:



IP RTP Prioritization is an add-on to WFQ to support low-delay propagation of packets.
It can be used for UDP traffic only.
IP RTP Prioritization also polices the high priority traffic to prevent starvation of other queues.



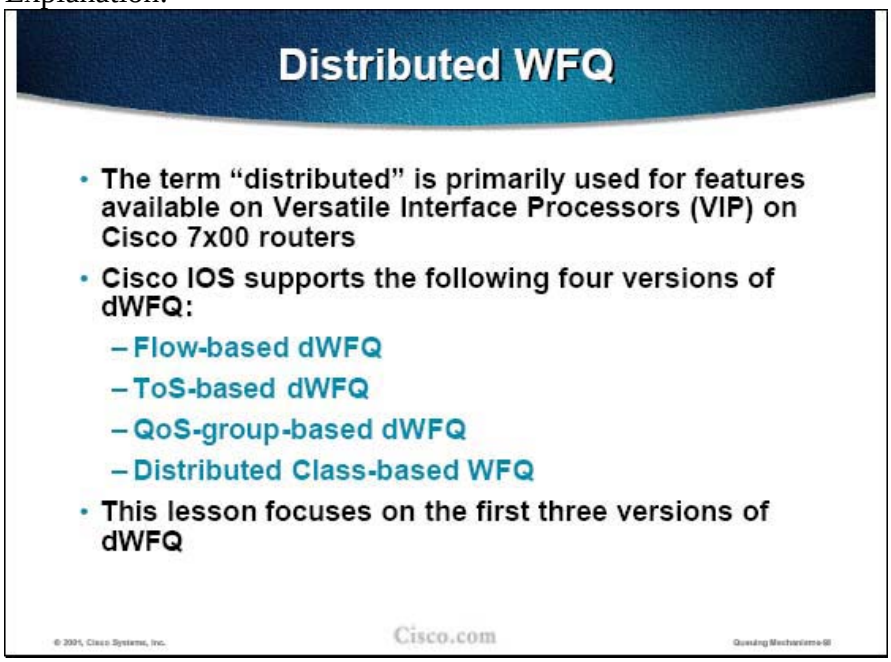
IP RTP Prioritization supports one high priority queue. Packets from this queue are scheduled ahead of other packets as long as they are within the configured rate.
Excess packets are dropped.
Sources: Cisco Queuing Mechanisms, Pages 3-134, 3-135

QUESTION 98
Which of the following are versions of distributed WFQ (dWFQ)? (Choose all that apply.)

A. CAR-based dWFQ
B. QPPB-based dWFQ
C. flow-based dWFQ
D. ToS-based dWFQ
E. DiffServ-based dWFQ
F. precedence-based dWFQ

Answer: C, D

Explanation:



The distributed versions of Weighted Fair Queuing are implemented on Cisco 7x00 series routers with Versatile Interface Processors (VIPs). There are four different versions of distributed WFQ, three of which are discussed in this module:
Flow-based dWFQ or simply dWFQ
ToS-based dWFQ
QoS-group-based dWFQ or QoS-based dWFQ
VIP is basically a router within a router. It has its own processor and its own (different) version of the IOS. Most features implemented on VIPs have different functionality than those available on the Route Switch Processor (RSP).
Source: Cisco Queuing Mechanisms, Page 3-86

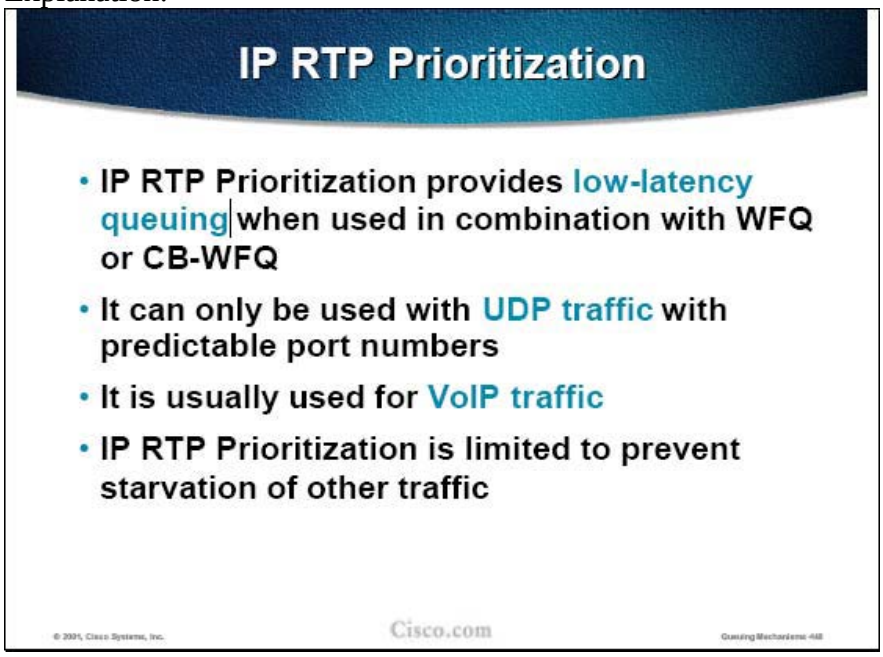
QUESTION 99
The newly appointed Certkiller trainee technician wants to know what the difference is between Low Latency Queuing (LLQ) and IP Real-Time Transport Protocol (RTP) priority. What will your reply be?

A. LLQ is not limited to defining traffic flows when making use of UDP port numbers.
B. IP RTP Priority has the ability to specify traffic matches based on DSCP whereas LLQ

cannot.
C. LLQ can accommodate voice traffic that is not supported in IP RTP Priority configurations.
D. LLQ priority queues suffer from "starvation" of low priority traffic due to preferential treatment of the high priority queue.

Answer: A

Explanation:



IP RTP Prioritization is an add-on to WFQ to support low-delay propagation of packets. It can be used for UDP traffic only.
IP RTP Prioritization also polices the high priority traffic to prevent starvation of other queues.
Source: Cisco Queuing Mechanisms, Page 3-134

QUESTION 100
Which of the following represent important advantages of applying QoS to IP networks? (Choose all that apply.)

A. QoS manages packet loss during periods of bursty congestion.
B. QoS facilitates the integration of differing traffic types such as voice, video, and data into a single infrastructure.
C. QoS is capable of preoviding performance enhancements for commercial application issues such as server sizing and tuning.
D. QoS allows the control usage patterns of network applications.
E. QoS is capable of solving traffic problems on low bandwidth, high-latency, high-loss WAN links.

Answer: A, B, E

QUESTION 101
What are three features of CBWFQ? (Choose three.)

A. CBWFQ supports two drop methods: tail drop and WRED.
B. CBWFQ support up to 4096 dynamic queues.
C. CBWFQ provides fixed-delay guarantees.
D. If some queues do not need the bandwidth, the bandwidth is spread across the other classes.
E. CBWFQ provides fixed, minimum-bandwidth guarantees.
F. CBWFQ does not require manual traffic-classification configurations.

Answer: A, D, E
Reference: Cisco Press - DQOS Exam Certification Guide p.273

QUESTION 102
Which configuration command applies QoS features to a particular traffic class?

A. class-map
B. traffic-map
C. policy-map
D. table-map

Answer: C

Explanation:
Using policy-map command you can associate the traffic class with one or more QOS features using the policy-map command.
Reference: Introduction to IP QoS (Course) p.8-5

QUESTION 103
When configuring CB-shaping and using shape adaptive command, how should the min-rate be configured?

A. The min-rate should be equal to or greater than the minimum bandwidth guarantee for that traffic class.
B. The min-rate should be configured to match the bandwidth configured on the physical interface.
C. The min-rate should be configured as the PIR/32 or 1500 bytes. Whichever is grater. Whichever is greater.
D. The min-rate should be configured as the CIR/8.

Answer: A

Explanation:

Min-rate parameter specifies the minimum shaping rate allowed. It should be greater than the guarantee level.

QUESTION 104
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know what global synchronization is. What will your reply be?

A. It is the purposeful dropping of 1 packet per TCP connection, to quickfix congestion on all TCP connections.
B. It is the process of selectively discarding TCP using packets, based on IP Precedence weighting, to reduce congestion.
C. It is the side effect of dropped packets on many simultaneous TCP connections, which causes network utilization to fluctuate between congestion state and an underutilized state.
D. It is typical of Internet performance that has been improved with advanced TCP features (i.e., Slow Start, Congestion Avoidance, and Fast Retransmit)

Answer: C

Explanation:
If the receiving router drops all traffic that exceeds the queue limit, as is done by default (with tail drop), many TCP sessions then simultaneously go into slow start.
Consequently, traffic temporarily slows down to the extreme and then all flows slow-start again. This activity creates a condition called global synchronization.
Reference: Introduction to IP QoS p.5-5

QUESTION 105
What is the TCP measurement of the delay for a packet to get the receive and then back to the send called?

A. window size
B. transit delay
C. transit window delay
D. round-trip time
E. propagation delay
F. serialization delay

Answer: D

Explanation:
Round-trip time equals a sum of all propagation, processing and queuing delay in the path.
Propagation delay is fixed, processing and queuing delay are unpredictable in best-effort networks.
Reference: Introduction to IP QoS p.7

QUESTION 106
Which of the following is valid about Low Latency Queuing (LLQ) but invalid when considering IP RTP priority?

A. It reserves and guarantees a configured amount of bandwidth.
B. It can be used for both TCP and UDP traffic types.
C. It is useful for RTP-based voice and video traffic.
D. It can match a range of UDP port numbers and provide lower latency for that traffic.
E. None of the above.

Answer: B

QUESTION 107
Name two sensitivities that Voice traffic has that data traffic is not necessarily affected by. (Choose two)

A. EMI
B. RFI
C. TPI
D. Jitter
E. Delay
F. Noise

Answer: D, E

QUESTION 108
What are two common problems for video in the absence of QoS? (Choose two)

A. Dimmer video images.
B. Jerky video image movement.
C. Fuzzy edges on video images.
D. Unsynchronized audio and video.

Answer: B, D

Explanation:
Today the Internet is serving a large population of all walks of life. The Internet has also grown in its service offering. Users are using the Internet to view static or dynamic information, transmit voice and video, shop, play etc.
Along with these new applications of the Internet come some demands on the service(s) it provides:
1) Some applications are slow
2) Video broadcast or conferencing may have bad picture quality or appear jerky
3) Voice sessions may have bad voice quality or periods of silence
4) Critical transactions may take too long (too many seconds)

5) Bulk transfers take too long (too many hours)
Reference: Introduction to IP QoS p.3

QUESTION 109
Which three are congestion management techniques according to the Cisco QoS Framework? (Choose three)

A. CQ
B. PQ
C. LLQ
D. CAR
E. NBAR

Answer: A, B, C
Reference: Cisco Press - DQOS Exam Certification Guide p.104

QUESTION 110
What is true of LLQ but not true of IP RTP priority?

A. Reserves a configured amount of bandwidth.
B. Is useful for RTP-based voice and video traffic.
C. Can be used for both TCP and UDP traffic types.
D. Can match a range of UDP port numbers and provide lower latency for that traffic.

Answer: C

QUESTION 111
Which IOS queuing features will ensure a configured amount of bandwidth to a particular class of traffic?

A. CAR
B. CQ
C. LLQ
D. WFQ
E. CBWFQ
F. PQ

Answer: B, C, E

Explanation:
CQ provides specific percentage of bandwidth for each flow. LLQ and CBWFQ can guarantee that the flow with the biggest priority would never starve and the bandwidth would be guaranteed it.

QUESTION 112
Which subcommand will you advice the new Certkiller trainee technician to use

when configuring LLQ on a Frame Relay interface?

A. frame-relay ip rtp priority class-map
B. priority map-class
C. priority policy-map
D. frame-relay ip rtp priority interface
E. priority class-map

Answer: C

Explanation:
To give priority to a class of traffic belonging to a policy map, use the priority policy-map class configuration command. To remove a previously specified priority specified for a class, use the no form of this command.
priority{bandwidth-kbps| percent percentage} [burst]
no priority {bandwidth-kbps| percent percentage} [burst]
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chap

---

QUESTION 113
Which of the following statements about NBAR is true?

A. NBAR is supported on multicast enabled interfaces
B. NBAR can match up to the 512 bytes in a packet payload
C. NBAR can classify application traffic by looking beyond the the TCP/UDP port numbers of a packet
D. NBAR can be used to classify output traffic on a WAN link where tunneling or encryption is used/

Answer: C
Page 185, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 114
Which mechanism does LLQ use to support real-time traffic?

A. IP RTP
B. RED
C. CBWFQ
D. PQ

Answer: D
Page 288-290, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 115
What s a drawback of the integrated services model of QoS deployment?

A. no service guarantees
B. limited scalability
C. requires complex QoS mechanisms on each router to implement the RSVP PHB
D. requires complex classification and marking of traffic at the network edge

Answer: B
The main drawback of IntServ as its limited scalability.

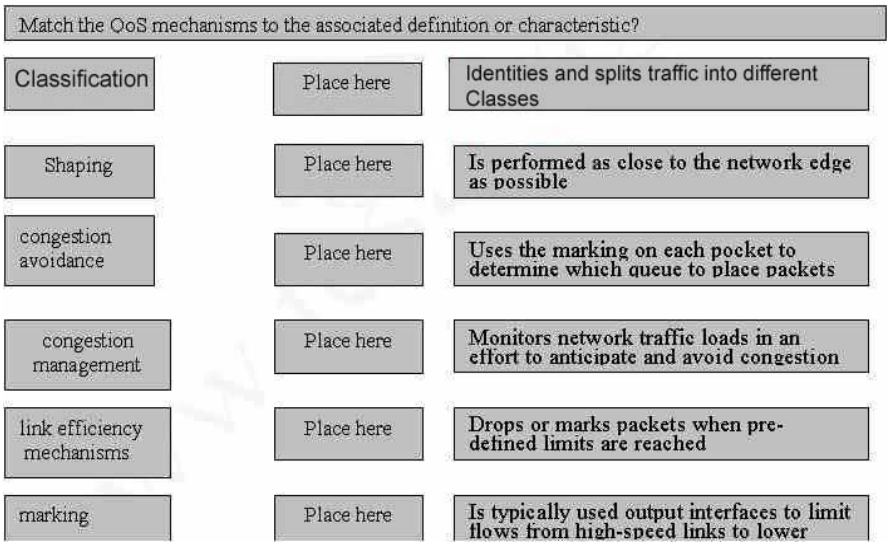
QUESTION 116
Which two statements regarding LLQ configuration are correct? (Choose two.)

A. The bandwidth command configures the required minimum bandwidth guarantee for the low-latency traffic.
B. The bandwidth command configures the required maximum bandwidth guarantee for the low-latency traffic.
C. LLQ only supports tail-drop for the low-latency queue.
D. LLQ only supports WFQ for the low-latency queue.
E. LLQ provides strict priority queuing for CBWFQ.
F. LLQ uses a congestion-aware policer to police the maximum bandwidth guarantee.

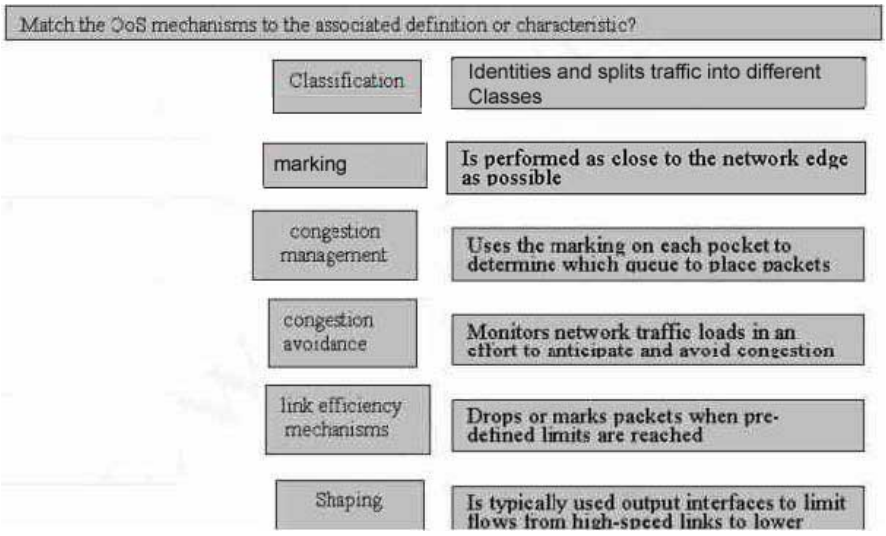
Answer: C, E

Explanation:
LLQ is not really a separate queuing tool, but rather a simple option of CBWFQ applied to one or more classes. CBWFQ treats these classes as strict-priority queues. In other words, CBWFQ always services packets in these classes if a packet is waiting, just as PQ does for the High queue.
Reference: DQOS Exam Certification Guide p.288

QUESTION 117
DRAG DROP



Answer:



QUESTION 118

Which four factors must be considered when determining the pre-call bandwidth requirement for voice traffic? (Choose four.)

A. router memory size and CPU speed
B. Use NBAR to classify voice bearer and control traffic
C. Codec type
D. Packetization interval
E. Layer 2 protocol overhead
F. Bandwidth required for he voice control (signaling) traffic

Answer: C, D, E, F

QUESTION 119

Which IOS queuing mechanism allows you to place packets at the front of the queue when you have a mission critical TCP application that will only be operational with

the lowest possible latency?

A. NBAR
B. CAR
C. LLQ
D. WFQ
E. CBWFQ
F. IP RTP Priority

Answer: C

Explanation:
The mission critical TCP application can be placed to the low-latency queue.
Like PQ, the LLQ scheduler always checks the low-latency queue first, and takes a packet from that queue. If there are no packets in the low-latency queue, the normal, unpublished scheduler logic applies to the other non-low-latency queue queues, giving them their guaranteed bandwidth.
Reference: Cisco Press - DQOS Exam Certification Guide p.289

QUESTION 120
Study the Exhibit below carefully:

```
class-map fred
match ip dscp af41

policy-map barney
class fred
bandwidth 30

class-map wilma
match ip dscp af41

policy-map betty
class fred
bandwidth 30
class wilma
priority 100


int s 0/0
ip addr 10.1.1.1 255.255.255.0

int s 0/1
ip address 10.2.2.2 255.255.255.0
service-policy output barney

int s 0/2
ip address 10.3.3.3 255.255.255.0
service-policy output fred

int s 0/3
ip address 10.4.4.4 255.255.255.0
service-policy output wilma

int s 0/4
ip address 10.5.5.5 255.255.255.0
service-policy output betty
```

What serial interface makes use of LLQ?

A. serial 0/0

B. serial 0/1
C. serial 0/2
D. serial 0/4

Answer: D

QUESTION 121
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know which IOS queuing features use a strict priority queue. What will your reply be? (Choose all that apply.)

A. CQ
B. LLQ
C. CAR
D. PQ
E. NBAR
F. WFQ

Answer: B, D

Explanation:
Both LLQ and PQ use a strict priority queue. PQ (priority queuing) is fully based on strict priorities and LLQ uses strict priority only for its low latency queue.

QUESTION 122
What are the functions of RSVP in an Admission Control environment? (Choose all that apply.)

A. RSVP must determine if the application requesting resources is eligible.
B. RSVP must guarantee bandwidth and delay.
C. The requesting RSVP station must ensure end-to-end RSVP availability.
D. RSVP must determine the availability and adequacy of resources for the reservation.

Answer: B, D

Explanation:
RSVP is used for applications where bandwidth and delay related guarantees are necessary. Typical application which use RSVP are:
-Voice over IP (Cisco phones, Microsoft NetMeeting, ...)
-MPLS Traffic Engineering.
RSVP also must provide resources reservation.
Reference: Introduction to IP QoS p.7-8

QUESTION 123
Which of the factors mentioned below is important to keep in mind when selecting Call Admission Control (CAC) methods to be deployed in your network?

A. type of PBX
B. CAR
C. E.164 standards
D. network topology
E. QoS mechanisms deployed

Answer: D
Reference: Page 8-76 CAC design Network Topology Considerations

---

QUESTION 124
What is a notable problem with weighted round-robin (WRR) queuing?

A. improper bandwidth allocation
B. no traffic prioritization
C. queue starvation
D. difficult implementation

Answer: A

Explanation:
Keep in mind that each port has a finite amount of buffer space to support the buckets. One queue will take all of the buffer space, for instance, two queues will divide the buffer space into two parts, three queues divide the buffer space into three parts, and so on. If the buffer space is too small, it will not be effective in momentarily holding the traffic before transport. Because nonpriority queues are serviced in either a round-robin or a Weighted Round-Robin manner, there is no guearantee that the traffic in the buffer is transported next. This limitation can lead to instaneous buffer overrun.

QUESTION 125
In most VPN tunneling, what is the classic QoS problem?

A. VPN overhead eliminates QoS processing time.
B. VPN adds too much delay to be used for voice.
C. The QoS information is encrypted in the packet being tunneled.
D. The QoS information is removed in the encryption process.

Answer: C

QUESTION 126
How does explicit congestion notification (ECN) work with Weighted Random Early Detection (WRED)?

A. ECN provides an additional marking option to WRED when the number of packets in queue is between the minimum and maximum thresholds.
B. ECN is an extension to WRED that provides support non-WRED devices.

C. ECN removes the tail-drop mechanism form WRED and replaces it with a dual leaky-bucket, congestion-management mechanism.
D. ECN applies the mark probability denominator to all packets identified in the class-map.

Answer: A

Explanation:
As with RED, WRED monitors the average queue depth in the router and determines when to begin packet drops based on the queue depth. When the average queue depth crosses the user-specified "minimum threshold, " WRED begins to drop packets (both TCP and UDP) with a certain probability. If the average queue depth ever crosses the user-specified" maximum threshold, " then WRED reverts to "tail drop, " where all incoming packets might be dropped. The idea behind using WRED is to maintain the queue depth at a level somewhere between the minimum and maximum thresholds, and to implements different drop policies for different classes of traffic.
Reference: Introduction to IP QoS p.5-15

QUESTION 127
How does NBAR differ from traditional TCP/UDP packet recognition?

A. NBAR queries each application directly
B. NBAR uses different port numbers than TCP/UDP
C. NBAR builds a database of packet types
D. NBAR looks into the payload for application clues

Answer: D
Page 185, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 128
DRAG DROP
Drag the correct description to the correct implementation model.

Answer:

Explanation:

1) Best-effort. The Internet was designed for best-effort, no-guarantee delivery of packets. This behavior is still predominant in today's Internet.
2) Integrated Services model. Introduced to supplement the best-effort delivery by setting aside some bandwidth for application that require bandwidth and delay guarantees. The Integrated Services model expects application to signal their requirements to the network. Resource Reservation Protocol (RSVP) is used to signal QoS requirements to the network.
3) Differentiated Services model. Added to provide more scalability in providing QoS to IP packets. The main difference is that the network recognizes packets (no signalling is needed) and provides the appropriate services to them.
Reference: Introduction to IP QoS p.18

QUESTION 129
Compressed Real-time Transport Protocol compresses the 40 byte IP/UDP/RTP header down to what size?

A. Usually 1 or 2 bytes
B. Usually 2 or 4 bytes
C. Usually 4 or 8 bytes
D. Usually 8 or 16 bytes
E. It varies based on the information contained in the header.

Answer: B

QUESTION 130
Which RED packet drop mode is used when the average queue size has reached or exceeded its maximum?

A. no drop
B. tail drop
C. random drop
D. full drop

Answer: B
Page 435, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 131
Which of the tools mentioned below will you find most helpful when designing or managing QoS? (Choose all that apply.)

A. CPC
B. QDM
C. IPM
D. CAC
E. QPM

F. SMS
G. All of the above

Answer: B, C, E, F

Explanation:
These four are management tools which Cisco provides to assist in managing the QoS policies and configuration in a network.
Reference: DQOS Exam Certification Guide p.102, 103

QUESTION 132
The QoS design and implementation process comprises of the following steps:
1. characterize network
2. implement policy
3. determine customer priorities/QoS policy
4. monitor network
What is the correct order for these steps?

A. 4, 1, 3, 2
B. 1, 3, 2, 4
C. 3, 1, 2, 4
D. 1, 2, 3, 4
E. 4, 3, 1, 2

Answer: C

Explanation:
The process begins with determining priorities - what traffic should get more bandwidth? Less loss, jitter, and delay? The policies, however, typically define classes of traffic in general terms; you need to know the specific of the traffic patterns so that you can configure the QoS tools to classify the traffic correctly. At Step 2, you characterize the traffic, which enables you to know how to configure the various classification features of the QoS tools. Then you can proceed with Step3, where you actually configure the QoS tools. Finally, you ceed to monitor the network (Step 4) to determine whether you met the stated policy goals you determined in Step 1. The process continues over time, with the quality of the QoS implementation improving with each cycle.
Reference: DQOS Exam Certification Guide p.669

QUESTION 133
Within a distributed call processing environment, what can you use to achieve call admission control across the WAN?

A. You can use a 720VXR to diversify the IPN1 traffic.
B. You can use a CiscoWorks RME package to keep lines clear.
C. You can use a gatekeeper.
D. You can use a H.333 Line card.

Answer: C

QUESTION 134
Which features can be used to police traffic according to the Cisco QoS Framework?

A. CQ
B. LLQ
C. CAR
D. NBAR
E. WRED

Answer: C

Explanation:
Only a few remaining mechanisms have marking capabilities:
1) Committed Access Rate (CAR), which is used for traffic policing
2) Class-based Policing, which is also used for traffic policing
3) Class-based Marking, which is used for classification and marking purposes only. It may however be combined with other mechanisms available with the Modular QoS CLI
Reference: Introduction to IP QoS p.2-46

QUESTION 135
What are the advantages of making use of NBAR as part of a classification and marking design? (Choose all that apply.)

A. It is able to match any TCP or UDP port number.
B. It is able to match packets based on application layer information
C. It has the ability to match QoS, Precedence, pr DSCP using NBAR.
D. It has the ability to match packets that are difficult to match with access lists.
E. All of the above.

Answer: B, D

Explanation:
NBAR can be used to look beyond layer 4 port numbers and inspect the actual payload. Also NBAR can be used to easily identify data which can be hard to configure access lists.
DQOS course notes:
NBAR can classify static port protocols. Although access control lists (ACL's) can also be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACL's.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a0080134add

---

QUESTION 136
Which two interface commands will enable precedence-based WRED when configuring WRED without using the MQC?

A. wred
B. random-detect prec-based
C. service-policy random-detect
D. random-detect
E. wred prec-based

Answer: B, D

Explanation:
Random-detect command:
1) Enables IP precedence basid WRED
2) Default service profile is used
3) Non-distributed WRED cannot be combined with fancy queuing - FIFO queuing has to be used.
4) WRED can run distributed on VIP-based interfaces (dWRED)
5) dWRED can be combined with dWFQ
Random-detect precedence command:
1) Changes RED profile for specified IP precedence value
2) Packet drop probability at maximum threshold is 1/mark-prob/dominator
3) Non-wieghted RED is achieved by using the same RED profile for all precedence values.
Reference: Introduction to IP QoS p.5-22, 5-23

QUESTION 137
Which IOS features will you advice the new Certkiller trainee technician to use to combat the effects of global synchronization? (Choose all that apply.)

A. GTS
B. LLQ
C. FRED
D. WRED
E. RSVP
F. WFQ

Answer: C, D

Explanation:
Weighted RED (WRED) and Flow-Based WRED (FRED) are the two congestion-avoidance tools available in IOS.

QUESTION 138
The newly appointed Certkiller trainee wants to know which Cisco IOS congestion

avoidance features use IP Precedence to affect the probability of whether or not a packet will be dropped. What will your reply be? (Choose all that apply.)

A. CAR
B. RED
C. FRED
D. WRED
E. NBAR
F. WFQ

Answer: C, D

QUESTION 139
The newly appointed Certkiller trainee wants to know which Cisco IOS congestion avoidance features specifically penalizes flows (such as UDP) that does not respond to drops. What will your reply be?

A. IP RTP priority
B. RED
C. WFQ
D. FRED
E. NBAR
F. WRED

Answer: A, D
Not D: WRED is not sensitive to flows.

QUESTION 140
Which of the following show commands will list the settings and counters for WRED behavior when you configure WRED using MQC?

A. show wred
B. show policy
C. show interface s0 random
D. show wred interface policy
E. show policy wred
F. show wred policy

Answer: B
Not C: There is no command show interface s0 random

QUESTION 141
Exhibit:
interface Fddi2/1/0
rate-limit input access-group rate-limit 100 8000000 80000
conform-action

transmit exceed-action drop
ip address 200.200.6.1 255.255.255.0
!
access-list rate-limit 100 00e0.34b0.7777
What is the result of the configuration shown in the exhibit on input traffic to the FDDI interface?

A. All input traffic on the FDDI interface is rate limited to 80 Mbps.
B. Traffic from MAC address 00e0.34b0.7777 is rate limited to 80 Mbps.
C. Traffic sent to the FDDI interface is dropped if it exceeds a rate of 512,000 bps.
D. Traffic sent from the MAC address 00e0.34.b0.7777 is dropped if it exceeds a rate of 512,000 bps
E. All traffic sent to the FDDI interface is accepted at 100 Mbps as long as it conforms to the excessive burst parameter.

Answer: B

QUESTION 142
Which command is used on Cisco IOS routers to enable Flow based WRED (FRED)?

A. router#(config)flow enable
B. router#(config)random detect
C. router#(config-if)flow enable
D. router#(config)random detect flow
E. router#(config-if)random detect flow

Answer: E

Explanation:
To enable flow-based WRED, use the ramdom-detect flow interface configuration command.
You must use this command to enable flow-based WRED before you can use the random-detect flow average-depth-factor and ramdom-detect flow count commands to further configure the parameters of low-based WRED.
Reference: Introduction to IP QoS p.5-44

QUESTION 143
How do you enable PGM on Cisco routers?

A. Router#(config) ip pgm
B. Router#(config) set pgm
C. Router#(config) ip pgm router
D. Router#(config-if) ip pgm router
E. Router#(config-if) ip pgm enable

Answer: D

Explanation:
To enable Pragmatic General Multicast (PGM) Router Assist and thereby allow PGM to operate more efficiently on the router, use the ip pgm router interface configuration command. To disable PGM Router Assist for the interface, use the no form of the command.
ip pgm router
no ip pgm router
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a00

QUESTION 144
What is the main purpose of the Cisco IOS QPPB feature?

A. It provides flow-based WRED support to External BGP peers.
B. QPPB enables traffic shaping on BGP enabled WAN interfaces.
C. It conveys IP Precedence or QoS Group to destinations using BGP communities.
D. It allows non-CEF enabled routers to support QoS and BGP by tagging routes in the BGP table.
E. It provides QoS policy in BGP networks by allowing centralized QoS configuration confederations.

Answer: C

Explanation:
QoS Policy Propagation through BGP is a mechanism that can be split into two parts:
1) Policy propagation via BGP, where a QoS policy is encoded into a BGP attribute. BGP Communities are typically used to encode a QoS policy.
2) Marking of packets with IP precedence or QoS group based on the QoS policy learned via BGP.
BGP Policy is usually set on ingress routers (ingress for route propagation, egress for packet forwarding) in an Autonomous System. BGP then carries the information to other routers in the AS and translates (using a route map) this information into IP precedence or QoS group. Marking is then enabled on per-interface basis.
Reference: Introduction to IP QoS p.2-23

QUESTION 145
What is the purpose of shaping traffic conditioners in IP QoS?

A. Shaping reorders transmit queues to offer priority service to specific traffic flows.
B. Shaping is a non-buffer based solution that drops packets above a specified burst rate.
C. Shaping techniques monitor network traffic loads in an effort to anticipate and avoid congestion.
D. Shaping uses packet re-write capabilities to sort traffic and maintain specific data rates for classified traffic.

E. Shaping avoids delays by smoothing out speed mismatches in the network and by limiting transmission rates.

Answer: C

Explanation:
If the traffic exceeds the contract, one option is to shape the traffic. Shaping just means to buffer or queue the traffic, slowing it down, so that the resulting sending rate is withing the contract.
Reference: DQOS Exam Certification Guide p.130

QUESTION 146
When configuring Weighted Random Early Detection (WRED), what is a potential problem that could arise if the difference between the maximum threshold and the minimum threshold is too small?

A. Too many packets could be dropped resulting in global synchronization.
B. The network could become overly congested because not enough packets are dropped as traffic levels increase.
C. The only effect of these settings is that traffic utilization peaks are greatly reduced as smaller amounts of traffic are offered to the network.
D. This condition could never occur as the Cisco IOS forces users to configure a minimum distance setting between both the minimum and maximum threshold.
E. The WRED mechanism might not recognize the maximum threshold has been hit if it is configured too close to the minimum threshold.
The result would be unmanaged congestion.

Answer: A

Explanation:
The probability of a packet being dropped is based on three configurable parameters:
1) Minimum threshold - When the average queue depth is above the minimum threshold, RED starts dropping packets. The rate of packet drop increases linearly as the average queue size increases, until the average queue size reaches the maximum threshold.
2) Maximum threshold - When the average queue size is above the maximum threshold, all packets are dropped. If the difference between the maximum threshold and the minimum threshold is too small, many packets might be dropped at once, resulting in global synchronization.
3) Mark probability denominator - This is the fraction of packets dropped when the average queue depth is at the maximum threshold.
Reference: Introduction to IP QoS p.5-9

QUESTION 147
What are two features that allow AutoQos to recognize voice traffic? (choose two)

A. a new QoS tag unique to phones

B. trust boundaries to allow the switch to track IP phones on the network
C. CallManager device table queries
D. IP phone registration with each AutoQoS server
E. automatic configuartion of an MQC class for voice signalling traffic

Answer: B, E
Page 2,12, Cisco AutoQoS White Paper,
http//www.cisco.com/en/US/tech/ CK5 43/ CK7 59/technologies_white_paper09186a00801348bc.shtml

---

QUESTION 148
In CBWFQ, class weights can be applied by using which three options?

A. DSCP value from the CoS-to-DSCP map in the class-map statement
B. DSCP value in policy-map
C. bandwidth in kpbs
D. percentage of bandwidth on the configured interface
E. percentage of available bandwith

Answer: B, C, E
Page 276, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 149
Why is it necessary to map L2 QoS marking to L3 QoS marking?

A. because L2 QoS marking may not cross the network end to end
B. because L2 QoS markings such as CoS are only local to the router or switch
C. because L2 QoS marking can only identify up to 8 traffic classes
D. because routers do not support L2 QoS marjings
E. because L2 Qos marking cannot be trusted

Answer: A

QUESTION 150
What are three QoS benefits that can be gained when trust boundaries are extended from the distribution layer to the access layer in a network? (Choose three.)

A. Traffic is classified and marked immediately
B. Traffic classification is verified by distribution and core layer of the network.
C. Classification and marking at the edge increases distribution layer router processing power
D. Classification and marking at the edge minimizes upstream congestion.
E. Classification and marking is accomplished as close to the destination as possible.

Answer: B, C, D

QUESTION 151
Why is ECN considered an extension to WRED?

A. Instead of dropping packets, ECN marks them when the average queue length exceeds the threshold value.
B. ECN drops all packets when the average queue length is exceeded.
C. ECN drops only marked packets before entering them in the queue.
D. Because of tail dropping. ECN is identical to the way the WRED handles the queue buffering.

Answer: A

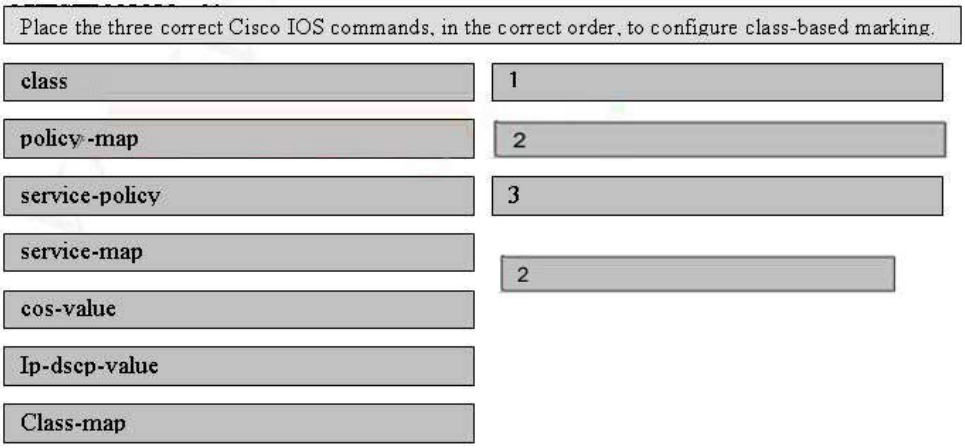
QUESTION 152
What are two benefits of using WRED to provide congestion management? (Choose two.)

A. Queue levels can be maintained somewhere between the minimum and maximum thresholds.
B. Lower priority traffic can selectively be discarded when the Interface becomes congested.
C. The average queue length is monitored and packets begin dropping only when the maximum threshold has been reached.
D. Statistically, more packets are dropped from small users than large users to preserve high flow queues.
E. The selective dropping capability is especially helpful in networks that support voice traffic.

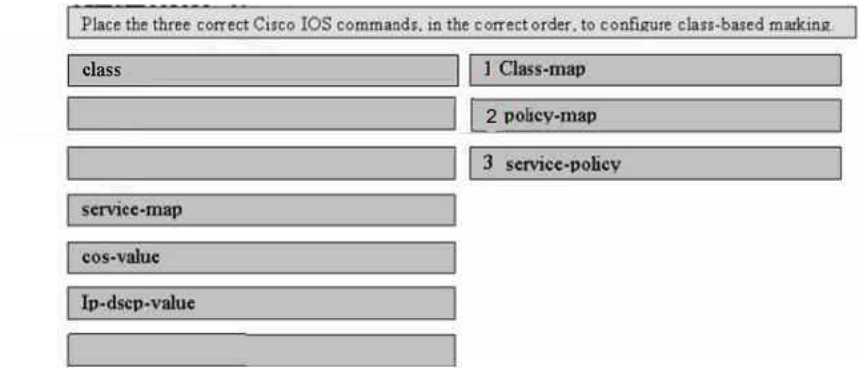
Answer: A, B

Explanation:
A: The idea behind using WRED is to maintain the queue depth at a level somewhere between the minimum and maximum thresholds, and to implement different drop policies for different classes of traffic.
Reference: Introduction to IP QoS p.5-15

QUESTION 153
DRAG DROP



Answer:



QUESTION 154
What are two key advantages of the DiffServ model? (Choose two.)

A. It is highly scalable
B. It provides many possible levels of service
C. It provides completely guaranteed quality of service
D. It works seamlessly with very little network configuration
E. It reserves bandwidth explicitly for each level of service

Answer: A, B

Explanation:
The Differentiated Services (DiffServ) model describes services associated with traffic classes. Traffic classes are identified by the value of the DiffServ Code Point (DSCP replaces IP precedence in the ToS field of the IP header).
The main goal of the DiffServ model are to provide scalability and a similar level of QoS to the Int Serv model, without having to do it on a per-flow basis. The network simply identifies a class (not application) and applies the appropriate per-hop behavior (QoS mechanism)
Reference: Introduction to IP QoS (Course) p.34

QUESTION 155
Which class-based, policing-configuration option uses dual token buckets that fill simultaneously but at different rates based on the configured PIR and CIR?

A. single-rate, dual token buckets, class-based policing
B. multi-action, class-based policing
C. dual-rate, class-based, class-based policing
D. percentage-based, class-based policing
E. peak-rate, class-based policing
F. average-rate, class-based policing

Answer: C

QUESTION 156
What is the correct class-based marking configuration to remark (map) traffic marked as "CoS4" or "CoS5" to DSCP AF 31"?

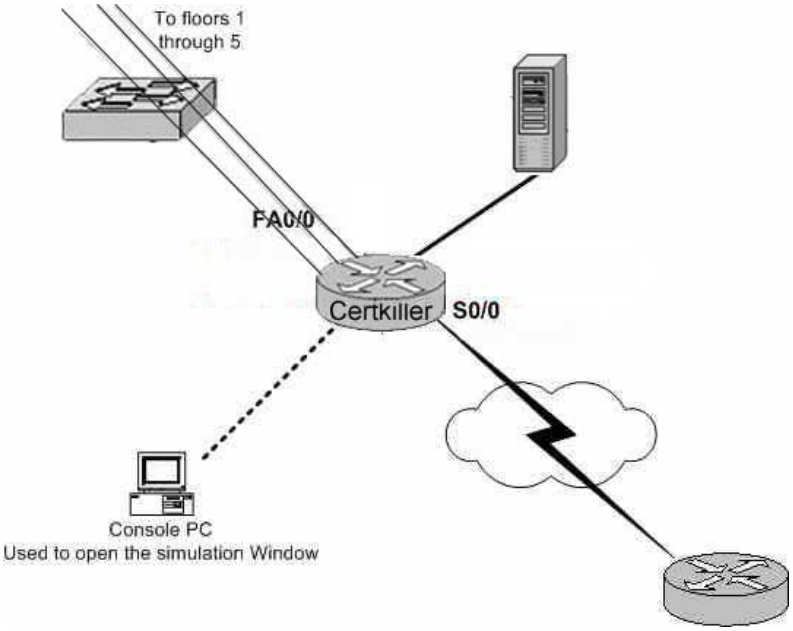
A. class.map cos4and5
Match cos 4 5
!
policy-map remark
class cos4and5
set dscp af31
B. class-map cos4and5
Match cos 4
Match cos 5
!
policy-map remark
class cos4and5
set dscp af31
C. class-map cos4
Match cos 4
!
class-map cos5
match cos5
!
policy-map remark
class cos4
class cos5
set dscp af31
D. class-map cos4
Match cos4
!
class-map cos5
match cos5
!

policy-map remark
class cos4 cos5
set dscp af31

Answer: B

Explanation:
Answer should be B
There are only two differences between answer A and answer B.
1) The first difference is the match statements in the class map. One is combined on one line and the other is on two separate lines. Both will work. So far both answers are correct.
2) Answer A uses the syntax "class.map" and answer B uses "class-map". Assuming there are no typos on the test, answer B is the correct syntax.

QUESTION 157
SIMULATION
Simulation exhibit:



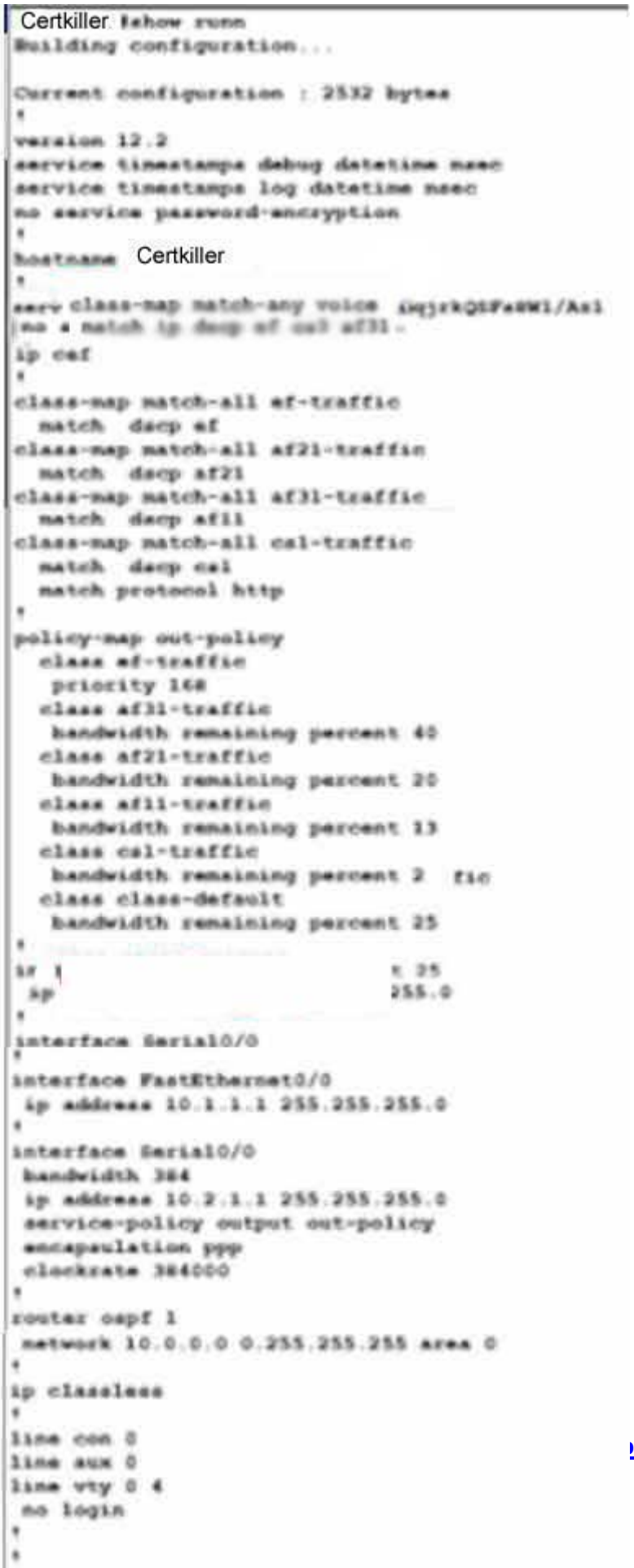
Note: You are required to evaluate the output the simulation to obtain the correct answer to this question.
Simulation output #1:

```
  where            List active connections
  write            Write running configuration to memory, network, or terminal
  x3              printers  privilege  processes
  x3              Write running configuration to memory,

Certkiller #show p?
policy-map  ppp  printers  privilege  processes  protocols

Certkiller #show policy-map
Policy Map out-policy
    Class ef-traffic
      Strict Priority
      Bandwidth 168 (kbps) Burst 4200 (Bytes)
    Class af31-traffic
      Bandwidth remaining 40 (%) Max Threshold 64 (packets)
    Class af21-traffic
      Bandwidth remaining 20 (%) Max Threshold 64 (packets)
    Class af11-traffic
      Bandwidth remaining 13 (%) Max Threshold 64 (packets)
    Class cs1-traffic
      Bandwidth remaining 2 (%) Max Threshold 64 (packets)
    Class class-default
      Bandwidth remaining 25 (%) Max Threshold 64 (packets)
Certkiller #
```

Simulation output #2:

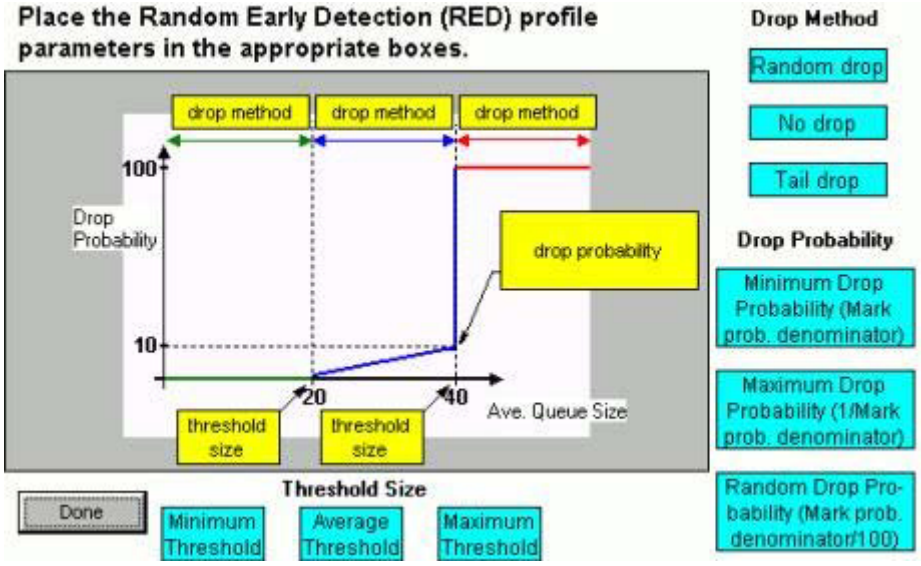

Certkiller #show runn
Building configuration...
Current configuration : 2532 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Certkiller
!
class-map match-any voice
ip cef
!
class-map match-all ef-traffic
match dscp ef
class-map match-all af21-traffic
match dscp af21
class-map match-all af31-traffic
match dscp af11
class-map match-all cs1-traffic
match dscp cs1
match protocol http
!
policy-map out-policy
class ef-traffic
priority 168
class af31-traffic
bandwidth remaining percent 40
class af21-traffic
bandwidth remaining percent 20
class af11-traffic
bandwidth remaining percent 13
class cs1-traffic
bandwidth remaining percent 2
class class-default
bandwidth remaining percent 25
!
ip address 10.1.1.1 255.255.255.0
!
interface Serial0/0
!
interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
!
interface Serial0/0
bandwidth 384
ip address 10.2.1.1 255.255.255.0
service-policy output out-policy
encapsulation ppp
clockrate 384000
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
no login
!
!

You work as a network administrator at Certkiller .com.
An upstream device has verified that HTTP packets are passing through the Certkiller router.
Why are no packets showing as matching the os1-traffic?

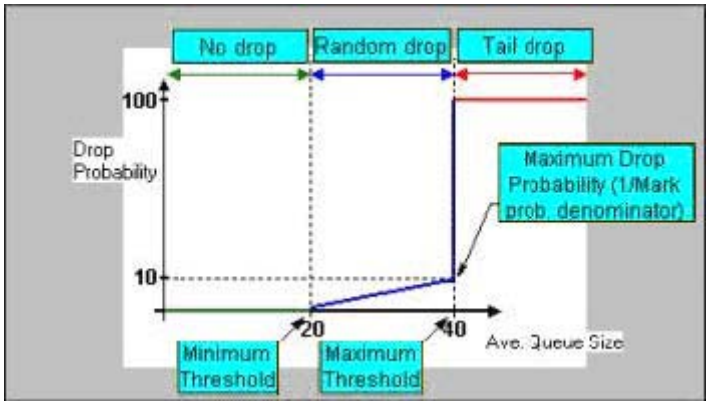
A. The policy-map out-policy configuration is incorrect.
B. The class-map cs1-traffic configuration is incorrect.
C. The service-policy is incorrectly applied to the serial 0/0 interface.
D. NBAR protocol discovery needs to be enabled on the serial 0/0 interface.
E. IP CEF must be disabled.

Answer: D

QUESTION 158
DRAG DROP
Place the Random Early Detection (RED) profile parameters in the appropriate boxes.

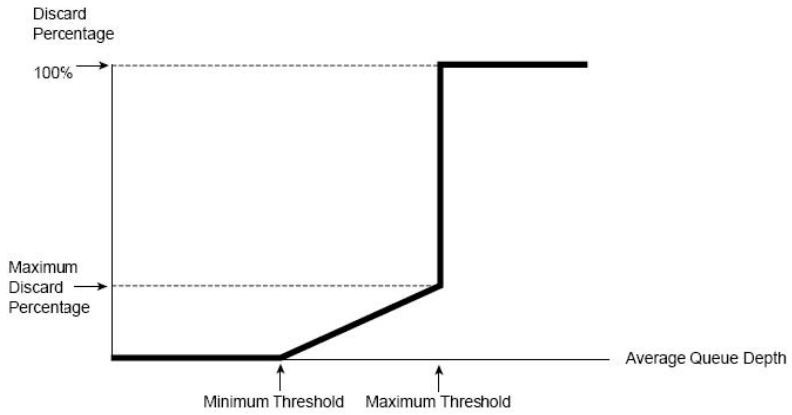


Answer:



Explanation:

Figure 6-6 *RED Discarding Logic Using Average Depth, Minimum Threshold, and Maximum Threshold*



You can set the maximum percentage of packets discarded by WRED by setting the mark probability denominator (MPD) setting in IOS. IOS calculates the maximum percentage using the formula 1/MPD. For instance, an MPD of 10 yields a calculated value of 1/10, meaning the maximum discard rate is 10 percent.
Source: Cisco DQOS Exam Certification Guide, Page 436

QUESTION 159
Within Modular QoS CLI, which three elements does a service policy contain? (Choose three)

A. Name
B. Policy type
C. Traffic class
D. QoS policies
E. Wildcard mask for matching policy criteria.
F. Instruction on how to evaluate the policy type.

Answer: A, C, D

Explanation:
A traffic policy contains three elements: a name, a traffic class (specified with the class command), and the QoS policies .
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00

QUESTION 160
You are using Modular QoS CLI to classify all packets except those that came in from a specific interface.
Which command should you use?

A. Match not interface
B. Match none interface
C. Match inverse interface
D. Match not input-interface

E. Match none input-interface
F. Match inverse input-interface

Answer: D

QUESTION 161
Under Modular QoS CLI's policies, the set command can be used to set_____.(Choose four)

A. ip dscp
B. atm-clp
C. qos-group
D. max-thresh
E. ip precedence

Answer: A, B, C, E

QUESTION 162
In the Differentiated Services model, what is the purpose of the Expedited Forwarding service class as defined in RFC 2598? (Select all that apply.)

A. Provides a traffic engineered path for packets to transit.
B. Ensures guaranteed bandwidth to a specific traffic class.
C. Provides for packet delivery with a specific reliable deliver guarantee.
D. Provides guaranteed packet forwarding with the lowest possible delay.
E. Ensures that packets traverse the network using the least loaded paths.

Answer: B, D

QUESTION 163
When using Modular QoS CLI to classify packets arriving from a specific MAC address, which command should you use?

A. Match mac
B. Match source
C. Match source-mac
D. Match source-address
E. Match source-address mac

Answer: E

Explanation:
Match source-address mac mac-address command classifies packets based on the source MAC address. This classification oprion can only be used on interfaces using MAC addresses (e.g. Ethernet, FastEthernet).
Reference: Introduction to IP QoS p.8-27

QUESTION 164
What are Packet Description Language Modules (PDLMs)

A. Modules containing the rules used by NBAR to recognize an application.
B. A client-server application NBAR queries for network application information.
C. Modules containing a scripting language used to list applications to be recognized by NBAR.
D. An application that searched network servers to list the applications to be recognized by NBAR.

Answer: A

Explanation:
Cisco uses a feature called packet descriptor language modules (PDLMs) to define new protocols that NBAR should match. When Cisco decides to add one or more new protocols to the list of protocols that NBAR should recognize, it creates and compiles a PDLM. You can then download the PDLM from Cisco, copy it into Flash memory, and add the ip nbar pdlm pdlm-name command to the configuration, where pdlm-name is the name of the PDLM file in Flash memory. NBAR can then classify based on the protocol information from the new PDLM.
Reference: DQOS Exam Certification Guide p.226

QUESTION 165
In which 3 scenarios can Cisco AutoQoS be extremely beneficial? (choose three.)

A. small-to-medium size businesses that have unlimited time and staffing skills to plan and deploy IP QoS services
B. large customer enterprises that need to deploy Cisco AVVID on a large scale, while reducing the cost, complexity, and timeframe for deployment and ensuring that the appropriate QoS for voice applications is being set in a consistent fashion.
C. international enterprises or service providers requiring QoS for VoIP in different regions of the world while little experience exists and where provisioning QoS remotely and across different time zones is difficult
D. service providers requiring a template-driven approach to delivering managed services and QoS for voice traffic to large numbers of customer-premise devices
E. large enterprises that need to deploy IPT and have a support staff capable of doing the design.

Answer: B, C, D
Page 2, Cisco AutoQoS White Paper,
http//www.cisco.com/en/US/tech/ CK5 43/ CK7 59/technologies_white_paper09186a00801348bc.shtml

QUESTION 166
DRAG DROP
Match the QoS characteristic with the matching QoS model

QoS characteristic, select from these

virtually unlimited scalability
the necessity for applications to signal their requirement to the network
packet recognition by the network (no signaling needed)
limited scalability
highly scalable
today's internet

QoS model

Best Effort
Integrated Services
Differentiated Services

Answer:

QoS model
Best Effort
virtually unlimited scalability
today's internet
Integrated Services
the necessity for application to signal their **requirement to the network**
limited scalability
Differentiated Services
packet recognition by the network (no signaling needed)
highly scalable

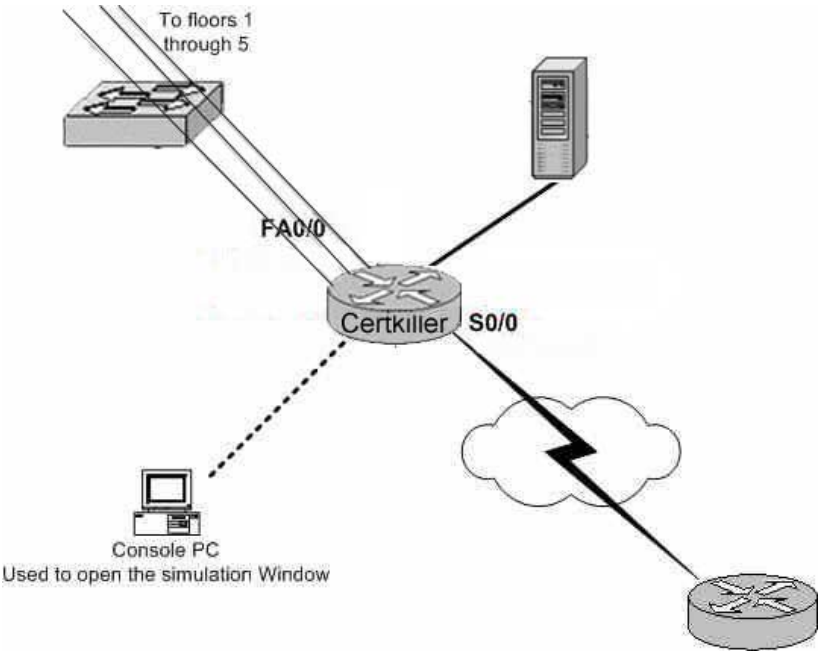
Explanation:
Page 777, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 167
How are IP precedence bits used in differentiated services to provide backward compatibility?

A. as the default PHB
B. as the class selector
C. as expedited forward bits
D. as the assured forwarding group

Answer: B
Page 129, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 168
SIMULATION
Simulation exhibit



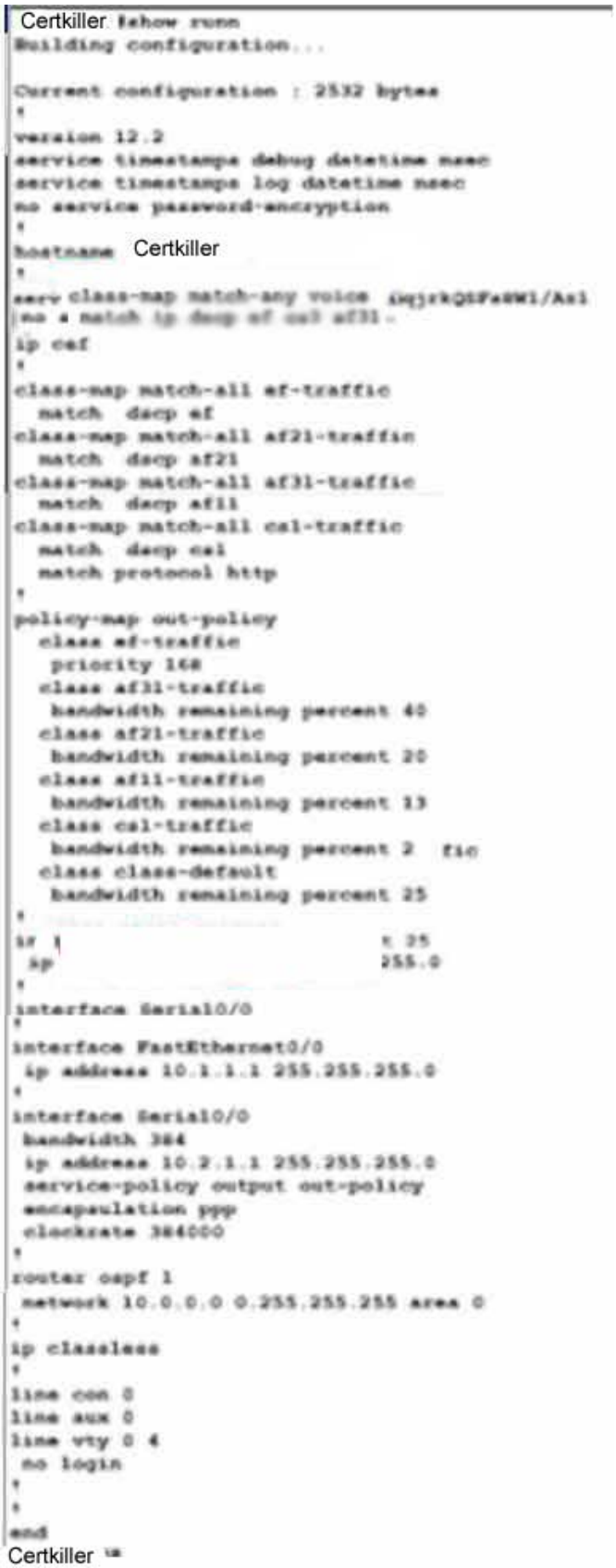
Note: You are required to evaluate the output the simulation to obtain the correct answer to this question.
Simulation output #1:

```
  where            List active connections
  write            Write running configuration to memory, network, or terminal
  x3              printers  privilege  processes
  x3             Write running configuration to memory,

Certkiller #show p?
policy-map  ppp  printers  privilege  processes  protocols

Certkiller #show policy-map
Policy Map out-policy
    Class ef-traffic
      Strict Priority
      Bandwidth 168 (kbps) Burst 4200 (Bytes)
    Class af31-traffic
      Bandwidth remaining 40 (%) Max Threshold 64 (packets)
    Class af21-traffic
      Bandwidth remaining 20 (%) Max Threshold 64 (packets)
    Class af11-traffic
      Bandwidth remaining 13 (%) Max Threshold 64 (packets)
    Class cs1-traffic
      Bandwidth remaining 2 (%) Max Threshold 64 (packets)
    Class class-default
      Bandwidth remaining 25 (%) Max Threshold 64 (packets)
Certkiller #
```

Simulation output #2:



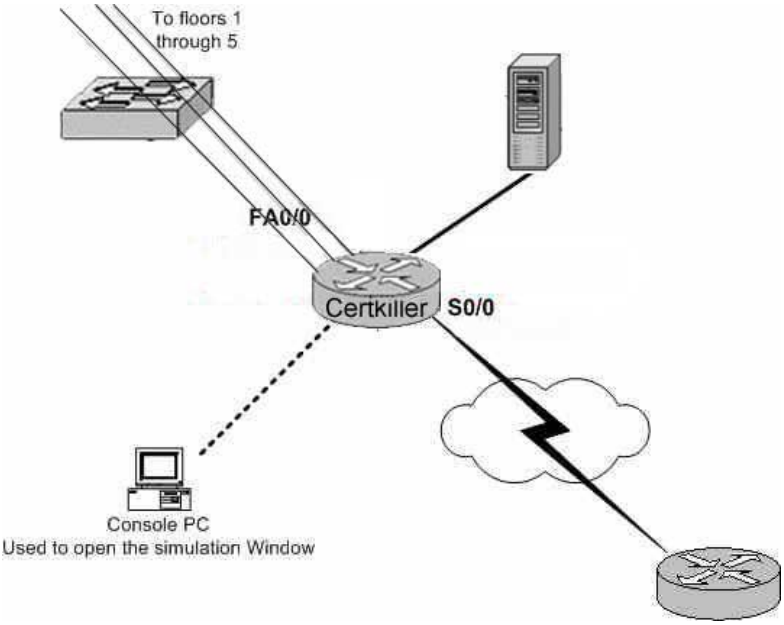
You work as a network administrator at Certkiller .com.

Which QoS method is applied to the serial 0/0 interface on the Certkiller router?

A. LLQ
B. CBWFG
C. LLQ + CB-WRED
D. CBWFQ + CBWRED
E. CB Policing
F. CB Shaping

Answer: A

QUESTION 169
SIMULATION
Simulation exhibit:



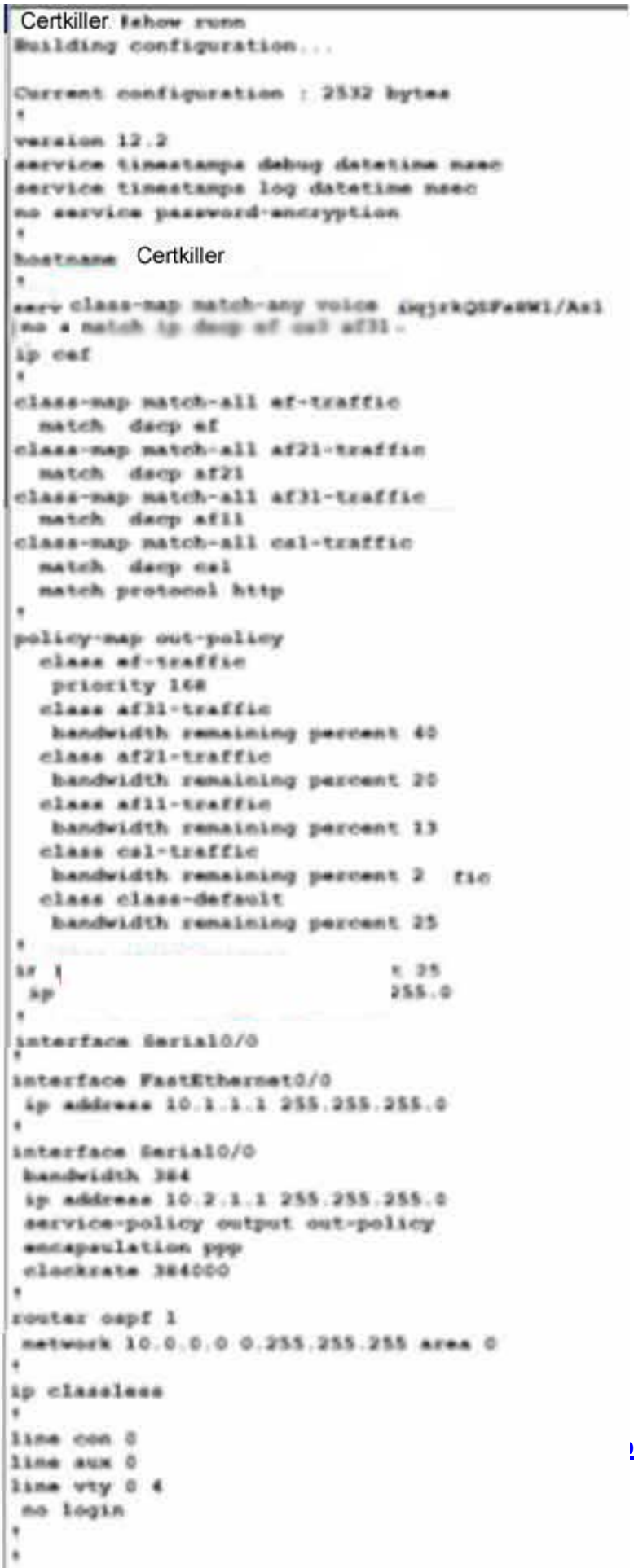
Note: You are required to evaluate the output the simulation to obtain the correct answer to this question.
Simulation output #1:

```
  where            List active connections
  write            Write running configuration to memory, network, or terminal
  x3              printers  privilege  processes
  x3             Write running configuration to memory,

Certkiller #show p?
policy-map  ppp  printers  privilege  processes  protocols

Certkiller #show policy-map
Policy Map out-policy
    Class ef-traffic
      Strict Priority
      Bandwidth 168 (kbps) Burst 4200 (Bytes)
    Class af31-traffic
      Bandwidth remaining 40 (%) Max Threshold 64 (packets)
    Class af21-traffic
      Bandwidth remaining 20 (%) Max Threshold 64 (packets)
    Class af11-traffic
      Bandwidth remaining 13 (%) Max Threshold 64 (packets)
    Class cs1-traffic
      Bandwidth remaining 2 (%) Max Threshold 64 (packets)
    Class class-default
      Bandwidth remaining 25 (%) Max Threshold 64 (packets)
Certkiller #
```

Simulation output #2:


Certkiller #show runn
Building configuration...
Current configuration : 2532 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Certkiller
!
class-map match-any voice
ip cef
!
class-map match-all ef-traffic
match dscp ef
class-map match-all af21-traffic
match dscp af21
class-map match-all af31-traffic
match dscp af11
class-map match-all cs1-traffic
match dscp cs1
match protocol http
!
policy-map out-policy
class ef-traffic
priority 168
class af31-traffic
bandwidth remaining percent 40
class af21-traffic
bandwidth remaining percent 20
class af11-traffic
bandwidth remaining percent 13
class cs1-traffic
bandwidth remaining percent 2
class class-default
bandwidth remaining percent 25
!
ip address 10.1.1.1 255.255.255.0
!
interface Serial0/0
!
interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
!
interface Serial0/0
bandwidth 384
ip address 10.2.1.1 255.255.255.0
service-policy output out-policy
encapsulation ppp
clockrate 384000
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
no login
!
!

You work as a network administrator at Certkiller .com.
Which statement is accurate regarding the status of interface serial 0/0?

A. Congestion has occurred on the interface.
B. No congestion has occurred on the interface.
C. The queuing mechanism was not invoked on the interface.
D. The TxRing limit is set at 64 packets.

Answer: B

QUESTION 170
Your boss at Certkiller .com is curious about WRED (Weighted Random Early Detection. In particular she wants to know which QoS mechanism is implemented by WRED.
What should you tell Mrs. Bill?

A. dropping
B. metering
C. policing
D. queuing
E. shaping

Answer: A

Explanation:
WRED is dropping packet in the queue based on their weights to avoid conjestion.

QUESTION 171
You work as a network administrator at Certkiller .com. You have deployed link efficiency mechanisms on a WAN Link. Your trainee asks you why. (Select three.)

A. decrease delay
B. decrease jitter
C. increase link speed
D. increase throughput
E. decrease propagation delay

Answer: A, B, D

QUESTION 172
The CIO of Certkiller wants to know what allows the Differential Services model to be scaled to large networking environments. What will your reply be?

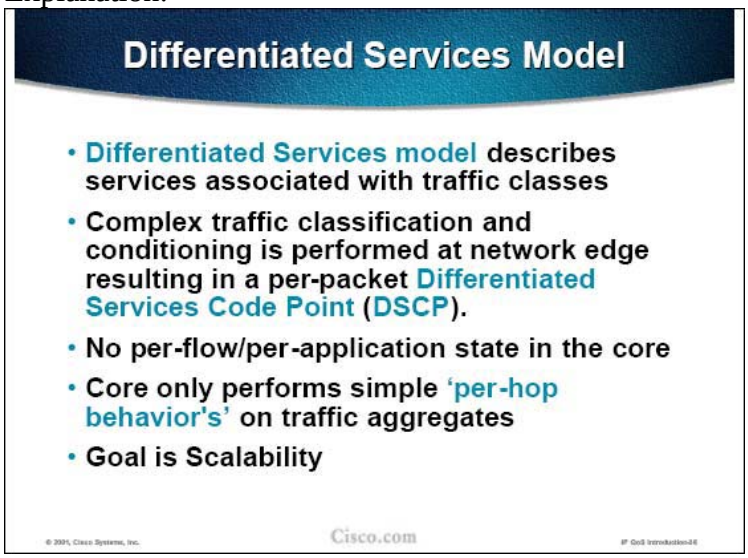
A. Differential services are accomplished through hop-by-hop application signaling.
B. The Differentiated Services model scales by providing per-flow state visibility to the core of the network.

C. Policing is not utilized in the Differentiated Services model providing to facilitate efficient expediting of high priority traffic flows.
D. It achieves scalability by implementing complex classification and conditioning requirements only at network boundary nodes.
E. In the Differentiated Services model, an explicit setup mechanism predefines all QoS parameters for the packet before it is transmitted.

Answer: D
Incorrect:

A. Core only performs simple 'per-hop behavior's' on traffic aggregates
B. No per-flow/per-application state in the core

Explanation:



Source: Cisco IP QoS Introduction, Page 34

QUESTION 173
At the network layer, IP packets are typically classified based on which three items? (Choose three.)

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

Answer: A, D, E
Reference: Introduction to IP QoS p.4-77

QUESTION 174
Which of the following are types of scheduling used by Cisco QoS features? (Choose all that apply.)

A. Round robin
B. Modified linear
C. Strict priority
D. Fair weighted
E. Weighted Random Early Detection (WRED)

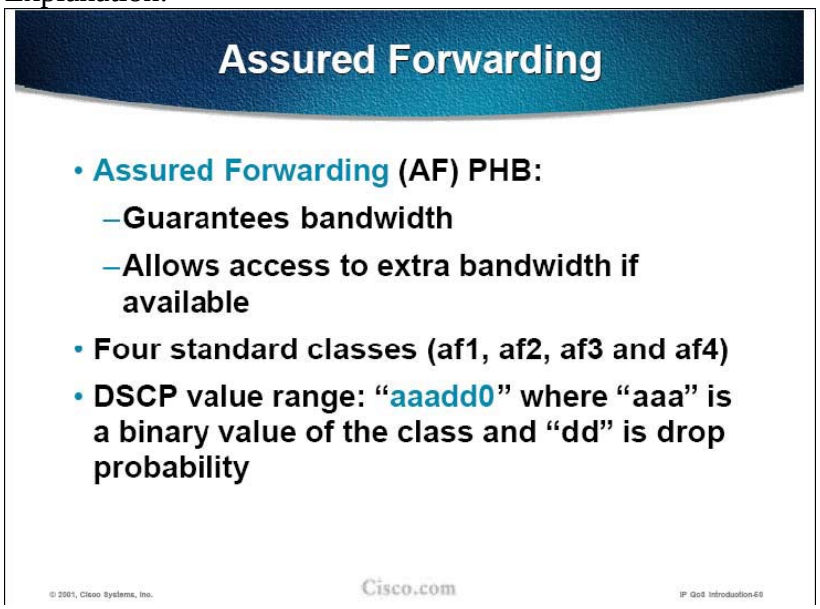
Answer: A, C, D

QUESTION 175
What is the default number of classes that Assured Forwarding (AF) have?

A. 1
B. 3
C. 4
D. 6
E. 8

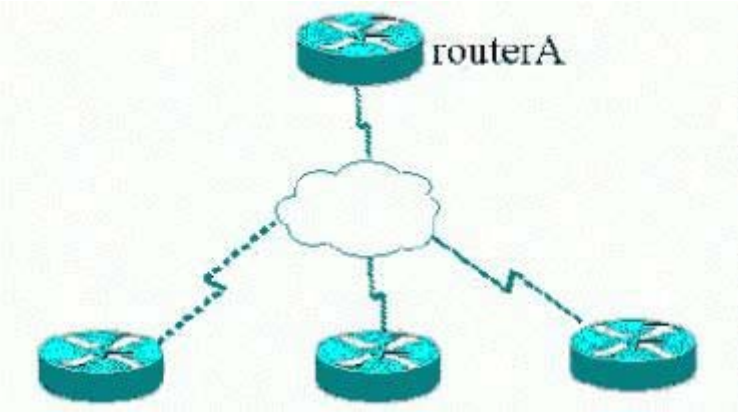
Answer: C

Explanation:



The Assured Forwarding PHB is identified based on the following parameters:
Guarantees a certain amount of bandwidth to an AF class
Allows access to extra bandwidth, if available
Packets requiring AF PHB should be marked with DSCP value "aaadd0"
where "aaa" is the number of the class and "dd" is the drop probability
There are four standard-defined AF classes. Each class should be treated independently and have bandwidth allocated based on the QoS policy.
Source: Cisco IP QoS Introduction, Page 49

QUESTION 176
Exhibit:



Central site router A has a single access link, which is a 512 Kbps link, with PVCs of CIR 256 K to each of three remote routers, namely routerB, routerC, and routerD. RouterB's output utilization on the PVC to routerA never exceeds an average of 100 Kbps. You have verified that it never even approaches 256 Kbps, even during short burts. Which two statements are true about fragmentation? (Choose two)

A. Since there is never congestion, there is no need for fragmentation.
B. The Frame Relay network inherently deals with congestion therefore no fragmentation is required,
C. There still may be large packets leaving routerB, so fragmentation may be beneficial to overcome serialization delay.
D. Congestion delay called "Egress Blocking" could occur for frames leaving the Frame Relay network, heading for routerA, so fragmentation at all the remote routers might help some frames to be interspersed.

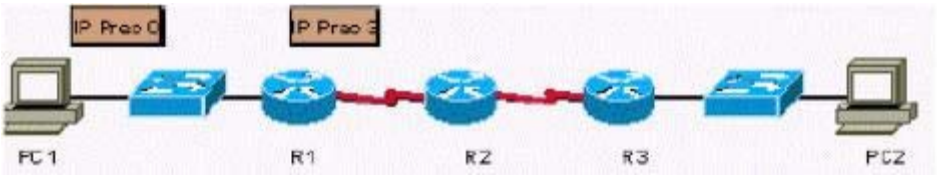
Answer: C, D

QUESTION 177
For very low-speed links (those with a link speed less than 768 K), it is necessary to use techniques that provide link fragmentation and interleaving of packets. This prevents voice traffic from being delayed behind large data frames and hence bounds jitter. What are two techniques that exist for this?

A. LECS for ATM links.
B. Multilink PPP (MLP) for Serial links.
C. FRF.12 for Frame Relay.
D. 1png for DSL links.

Answer: B, C

QUESTION 178
Exhibit:



PC1 sends a packet to R1. R1 forwards to R2, then R3, and finally R3 forwards the packet to the destination, PC2. R1 marks the packet with IP Precedence 3.
Which statement is true?

A. When classifying packets at Layer 3, only Layer 3 IP Precedence marking can be used.
B. R2 and R3 can perform QoS features that ignore the marked IP Precedence field in the packet.
C. R2 and R3 can only perform QoS features based on the IP Precedence field, since the packet had already been marked.
D. R2 can apply QoS features to the packet, and R3 can on ingress, but R3 cannot apply QoS features to the packet as it exists the Ethernet port on which PC2 resides.

Answer: B

QUESTION 179
From the list below, what is the most important piece to implement if you are considering a VoIP infrastructure?

A. Reinstallation of the PBX.
B. QoS
C. PSTN Regeneration costs.
D. POTS installation documentation.
E. A new Help Desk trained on Voice technologies.

Answer: B

QUESTION 180
Which tool from the list below can be applied to the Campus Switches to help eliminate traffic congestion?

A. QoS
B. LMI
C. PIM
D. DVRMP
E. CDP
F. RDP

Answer: A

QUESTION 181
Command exhibit: qos pre-classify

Your Certkiller .com trainee Sandra asks you what the purpose of the command displayed in the exhibit is.

A. To enable the IOS to copy the ToS field from the original IP header to the outer tunnel IP header.
B. To enable the IOS to copy the ToS field from the outer tunnel IP header to the outer tunnel IP header.
C. To enable the IOS to classify the packet based on the original IP header instead of the tunnel IP header.
D. To enable the IOS to classify the packet based on the outer tunnel IP header instead of the original IP header.
E. to enable class-based marking on tunnel interface
F. to enable class-based marking on IPSec crypto maps

Answer: C

Explanation:
For Layer 2 Forwarding(L2F) and Layer 2 Tunneling Protocol(L2TP) protocols, the qos pre-classify command is applied on the virtual template interface. L2TP clients belonging to identical virtual private dial-up network (VPDN) groups inherit the preclassification setting. The qos pre-classify command can be configured on a per-VPDN tunnel basis.
For IPSec tunnels, the qos pre-classify command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00

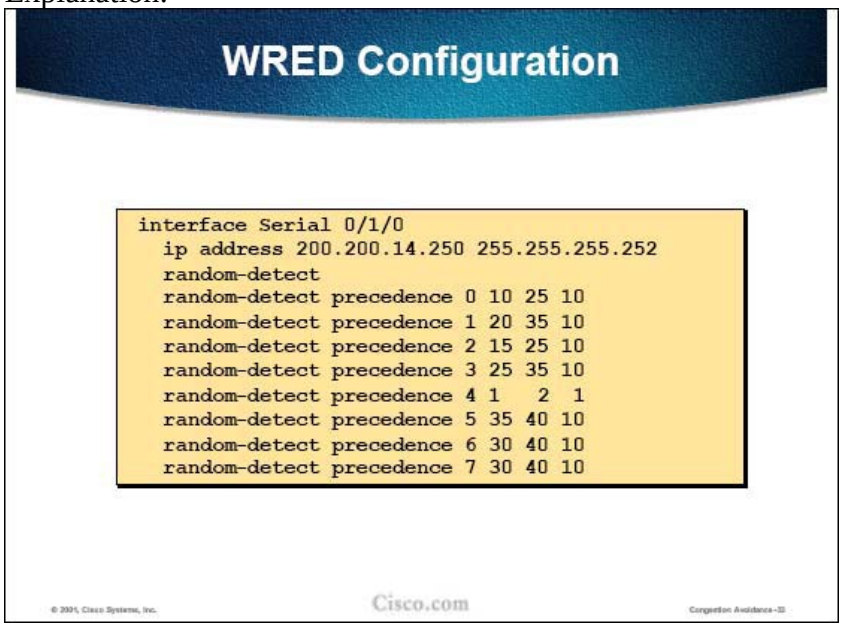
QUESTION 182
Study the Exhibit below carefully:
interface Serial 0/1/0
ip address 10.1.1.1 255.255.255.0
random-detect
random-detect precedence 0 1 2 1
random-detect precedence 0 10 20 10
random-detect precedence 2 15 20 10
random-detect precedence 3 20 30 10
random-detect precedence 4 25 30 10
random-detect precedence 5 30 40 10
random-detect precedence 6 35 40 50
random-detect precedence 7 35 40 100
random-detect exponential-weighted-constant 11
Based on the configuration in the exhibit, which statement is valid?

A. The drop probability of precedence 0 traffic is 100%.
B. The drop probability of precedence 1-5 traffic is 100%.
C. The drop probability of precedence 6 traffic is 100%.

D. The drop probability of precedence 7 traffic is 100%.

Answer: A

Explanation:



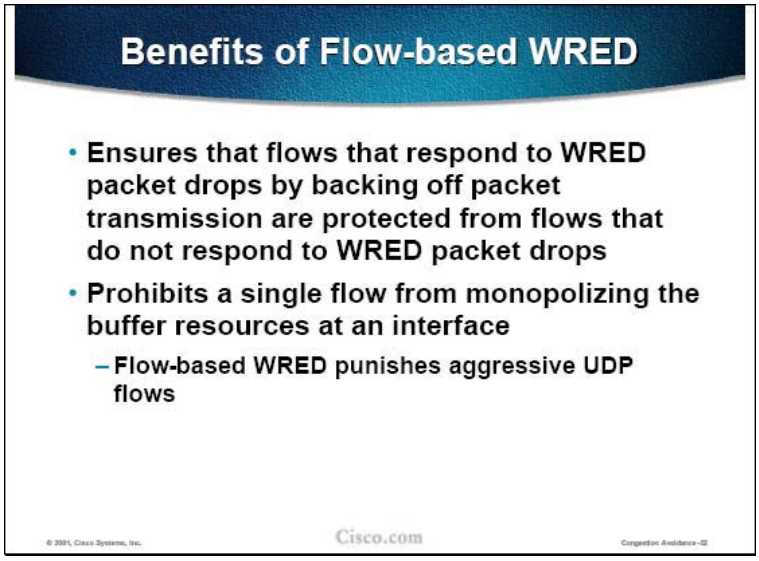
This configuration excerpt shows the implementation of the dropping policy, illustrated by the case study. The threshold values reflect the values chosen in the previous figure. Note that precedence 4 is not used to mark traffic in the case study network, so the drop probability of precedence 4 traffic is 100% (1 divided by 1 times 100%).
Source: Cisco Congestion Avoidance, Page 5-30

QUESTION 183
Why would a network administrator prefer to use Flow-based WRED (FRED) as opposed to standard Weighted Random Early Detection (WRED)?

A. In Cisco IOS, FRED is more user friendly when being configured as opposed to WRED.
B. FRED can classify packets using DSCP and WRED cannot.
C. FRED adds support for new protocol and traffic types including UDP.
D. With FRED, packets are not dropped indiscriminate of the kind of flows to which the packets belong.

Answer: D

Explanation:



FRED therefore has substantial benefits compared to WRED, as it can also be used in environments that do not exhibit a predominantly TCP-based traffic mix. FRED enables differentiated dropping between fragile and non-adaptive flows, in which the loss rate is higher with non-adaptive flows. This is something that WRED is unable to do, because it drops packets without regard to flow buffer usage. Therefore, FRED protects fragile and adaptive flows from non-adaptive flows, which may, in the case of RED, monopolize router queues in their path.
Source: Cisco Congestion Avoidance, Page 5-48

QUESTION 184
On what basis are packet drop decisions taken in an environment of Cisco implemented Weighted Random Early Detection (WRED)? (Choose all that apply.)

A. TCP window size
B. Interface buffer utilization
C. DSCP
D. IP precedence
E. Interface output queue size

Answer: C, D, E

Explanation:
WRED calculates the average queue depth just like RED, ignoring precedence, but it decides when to discard packets based on the precedence or DSCP value.
E: The queue depth is also taken into account, if the threshold is not reached, no packet is dropped.
Source: Cisco DQOS Exam Certification Guide, Page 438

QUESTION 185
The newly appointed Certkiller trainee technician wants to know which of the following steps are necessary when configuring policy-based routing on Cisco IOS routers. What will your reply be? (Choose all that apply.)

A. Assign the policy to an interface.
B. Enable local policy-based routing.
C. Enable fast-switched policy-based routing.
D. Specify the match criteria and resulting action.
E. Define a route map to be used by policy-based routing.

Answer: A, D, E

Explanation:
Example 3-7 *PBR Marking, VoIP as DSCP EF, Everything Else as BE*

```
ip route-cache policy
!
ip access-list extended VoIP-ACL
 permit udp any range 16384 32767 any range 16384 32767
!
int fastethernet 0/0
 ip policy route-map voip-routemap
!
route-map voip-routemap permit 10
 match ip address VoIP-ACL
 set ip precedence 5
!
route-map voip-routemap permit 20
set ip precedence 0
```

PBR uses route-map commands, along with match and set route-map subcommands, to classify and mark the packets. This configuration uses a route map named voip-routemap, which includes two clauses. The first clause, clause 10, uses a match command that refers to VoIP-ACL, which is a named IP ACL. VoIP-ACL matches UDP port numbers between 16,384 and 32,767, which matches all VoIP traffic. If the ACL permits a packet, the route map's first clause acts on the set command, which specifies that IP precedence should be set to 5.
The second route map clause, clause 20, matches the rest of the traffic. The route map could have referred to another IP ACL to match all packets; however, by not specifying a match statement in clause 20, all packets will match this clause by default. By not having to refer to another IP ACL to match all packets, less processing overhead is required. The set command then specifies to set precedence to zero.
The ip policy route-map voip-routemap command enables PBR on interface FA0/0 for incoming packets. Notice that the direction, input or output, is not specified, because PBR can only process incoming packets.
Source: Cisco DQOS Exam Certification Guide, Pages 203, 204

QUESTION 186
The newly appointed Certkiller trainee technician wants to know how per-VC Class-Based Weighted Fair Queuing (CBWFQ) works. What will your reply be?

A. A weight is assigned to the entire class, not to an individual flow.
Only a single class can be assigned to each VC.
B. A weight is assigned to the entire class, not to an individual flow.
Multiple classes can be assigned to each VC.
C. Each flow within a class is assigned a separate weight by CBWFQ.
Only a single class can be assigned to each VC.
D. Each flow within a class is assigned a separate weight by CBWFQ.

Multiple classes can be assigned to each VC.

Answer: C

QUESTION 187
Study the Exhibit below carefully:
<output omitted>
!
interface Ethernet0/0
ip address 161.24.52.1 255.255.255.0
traffic-shape group 101 1000000 125000 125000
!
interface Ethernet0/1
ip address 161.24.53.1 255.255.255.0
traffic-shape rate 5000000 625000 625000
!
access-list 101 permit udp any any
!
<output omitted>
In which way will the traffic leaving the router be affected by the configuration as illustrated? (Choose all that apply.)

A. All traffic leaving interface Ethernet 0/0 is rate limited to 1 Mbps.
B. All traffic leaving interface Ethernet 0/1 is rate limited to 5 Mbps.
C. All UDP traffic that enters interface Ethernet 0/0 is rate limited to 1 Mbps.
D. All non-UDP traffic that leaves interface Ethernet 0/0 can use the full line rate.
E. Excess burst capabilities have been disabled because the excess burst parameter has been configured to match the burst size.

Answer: B, D
Not E: E is not correct, to disable excess burst capability Be needs to be set to 0

Explanation:
traffic-shape group
To enable traffic shaping based on a specific access list for outbound traffic on an interface, use the traffic-shape group interface configuration command. To disable traffic shaping on the interface for the access list, use the no form of this command.
traffic-shape group access-listbit-rate [burst-size [excess-burst-size]]
no traffic-shape group access-list
Syntax Description

access-list	Number of the access list that controls the packets that traffic shaping is applied to on the interface.

bit-rate	Bit rate that traffic is shaped to (in bits per second). This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain.
burst-size	(Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the committed burst size contracted with your service provider.
excess-burst-size	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the excess burst size contracted with your service provider. The default is equal to the burst-size argument.

Usage Guidelines

Generic traffic shaping is not supported on ISDN and dialup interfaces. Is is also not supported on non-generic routing encapsulation (GRE) tunnel interfaces. Traffic shaping is not supported with flow switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

The traffic-shape group command allows you to specify one or more previously defined access list to shape traffic to on the interface. You must specify one traffic-shape group command for each access list on the interface.

The traffic-shape group command supports both standard and extended access lists.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

1. If the burst-size is not equal to zero, the interval is the burst-size divided by the bit-rate.
2. If the burst-size is zero, the interval is the excess-burst-size divided by the bit-rate.

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the frame-relay traffic-shaping command. For more information on Frame Relay traffic shaping, refer to the "Configuring Frame Relay" chapter in the Cisco IOS Wide-Area Networking Configuration Guide.

If traffic shaping is performed on a Frame Relay network with 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.

Examples

The following example enables traffic that matches access list 101 to be shaped to a certain rate and traffic matching access list 102 to be shaped to another rate on the interface:

```
interface serial 1
traffic-shape group 101 128000 16000 8000
```

traffic-shape group 102 130000 10000 1000
traffic-shape rateTo enable traffic shaping for outbound traffic on an interface, use the traffic-shape rate interface configuration command. To disable traffic shaping on the interface, use the no form of this command.
traffic-shape rate bit-rate[burst-size [excess-burst-size]]
no traffic-shape rate
Syntax Description

bit-rate	Bit rate that traffic is shaped to (in bits per second). This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain.
burst-size	(Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the committed burst size contracted with your service provider.
excess-burst-size	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the excess burst size contracted with your service provider. The default is equal to the burst-size argument.

Defaults
Traffic shaping is disabled.
Usage Guidelines
Generic traffic shaping is not supported on ISDN and dialup interfaces. Is is also not supported on non-generic routing encapsulation (GRE) tunnel interfaces. Traffic shaping is not supported with flow switching.
Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.
Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.
An interval is calculated as follows:
1. If the burst-size is not equal to zero, the interval is the burst-size divided by the bit-rate.
2. If the burst-size is zero, the interval is the excess-burst-size divided by the bit-rate.
Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the frame-relay traffic-shaping command. For more information on Frame Relay traffic shaping, refer to the "Configuring Frame Relay" chapter in the Cisco IOS Wide-Area Networking Configuration Guide.
If traffic shaping is performed on a Frame Relay network with 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.
Examples
The following example enables traffic shaping on serial interface 0 using the bandwidth required by the service provider:
interface serial 0
traffic-shape rate 128000 16000 8000
Source:
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a

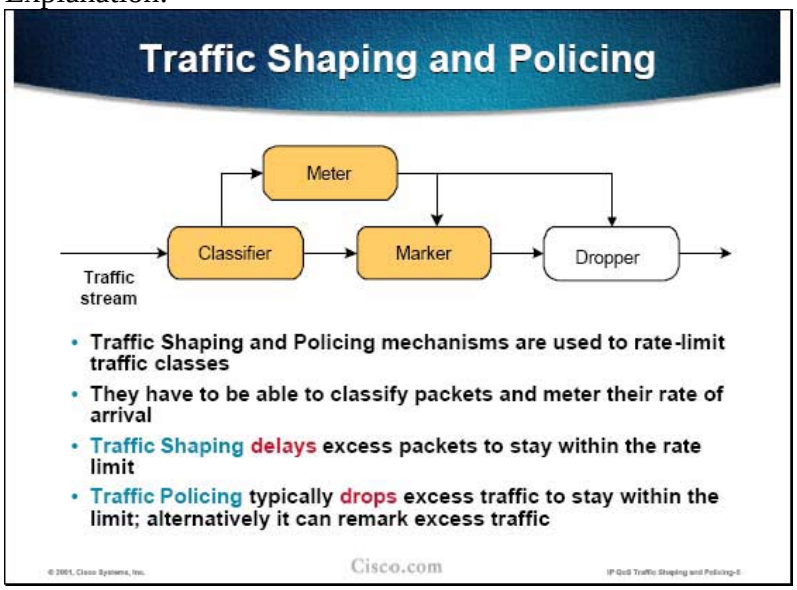
---

QUESTION 188
Which of the following QoS components will you find in both traffic shaping and policing? (Choose all that apply.)

A. meter
B. dropper
C. classifier
D. marker
E. shaper

Answer: A, C, D

Explanation:



Both shaping and policing mechanisms are used in a network to control the rate at which traffic is admitted into the network. Both mechanisms use classification, so they can differentiate traffic. They also use metering to measure the rate of traffic and compare it to the configured shaping or policing policy.
The difference between shaping and policing can be described in terms of their rate-limiting implementation:
Shaping meters the traffic rate and delays excessive traffic so that it stays within the

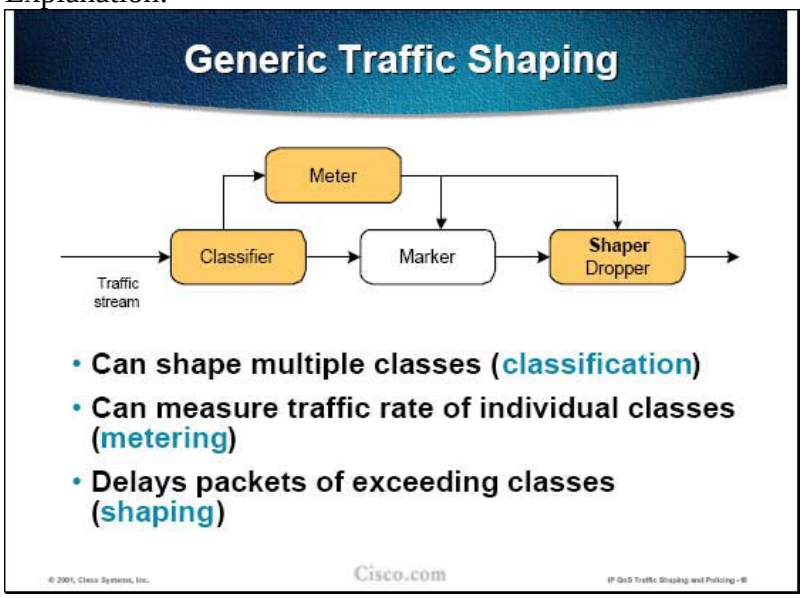
desired rate limit. With shaping, traffic bursts are smoothed out producing a steadier flow of data. Reducing traffic bursts helps reduce congestion in the core of the network.
Policing drops excess traffic in order to control traffic flow within specified limits. Policing does not introduce any delay to traffic that conforms to traffic policies. It can however, cause more TCP retransmissions, because traffic in excess of specified limits is dropped.
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-3

QUESTION 189
In which way is congestion managed when using Generic Traffic Shaping (GTS)?

A. Call Admission Control is performed on classified traffic to ensure allocated bandwidth is not exceeded.
B. It uses multiple traffic queues that are serviced in a round-robin fashion that promotes fairness and reduces congestion.
C. Strict priority is maintained for classified traffic and is policed through packet discard.
D. Random Early Detection (RED) is used to selectively drop packets and avoid congestion.
E. Outbound traffic is constrained to a particular bit rate using a token bucket mechanism.

Answer: E

Explanation:



Generic Traffic Shaping (GTS) shapes traffic by reducing the outbound traffic flow to avoid congestion. This is achieved by constraining traffic to a particular bit rate using the token bucket mechanism. GTS is applied on a per-interface basis and can use access lists to select the traffic to shape. It works with a variety of Layer-2 technologies, including Frame Relay, ATM, Switched Multi-megabit Data Service (SMDS) and Ethernet.
As shown in the block diagram, GTS performs three basic functions:

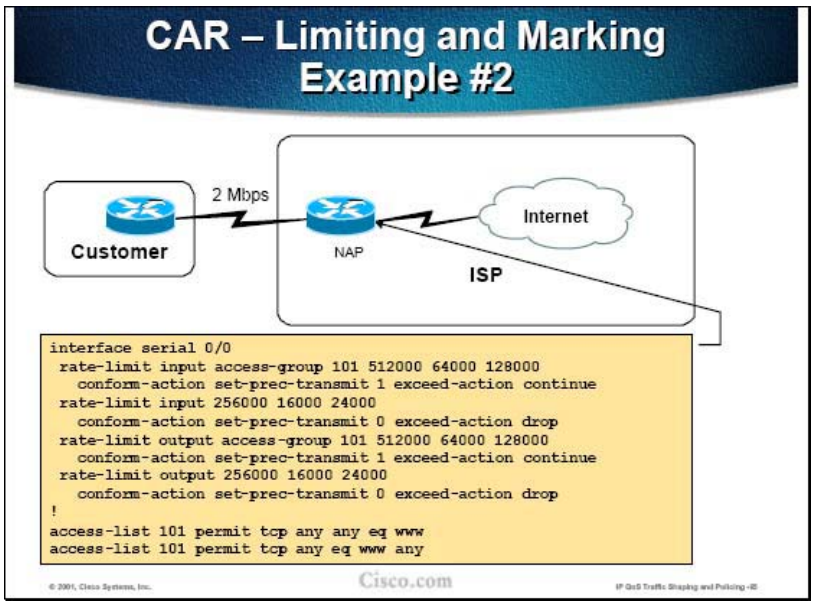
Classification of traffic, so that different traffic classes can have different policies applied to them
Metering, using a token-bucket mechanism, to distinguish between conforming and exceeding traffic
Shaping, using buffering, to delay exceeding traffic and shape it to the configured rate limit
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-15

QUESTION 190
Study the Exhibit below carefully:
interface Hssi0/0/0
description 45Mbps to R2
rate-limit output access-group 101 20000000 24000 32000
conform-action set-prec-transmit 5
exceed-action set-prec-transmit0
rate-limit output access-group 102 10000000 24000 32000
conform-action set-prec-transmit 5
exceed-action drop
rate-limit output 8000000 16000 24000
conform-action set-prec-transmit 5 exceed-action drop
ip address 10.1.0.9 255.255.255.0
!
access-list 101 permit tcp any any eq www
access-list 102 permit tcp any any eq ftp
Following the exhibit, what happens to WWW traffic sent out the HSSI interface?

A. WWW traffic is rate limited to 80 Mb.
Traffic exceeding the rate policy is dropped.
B. WWW traffic is limited to 10 Mb.
Conforming traffic is sent as IP precedence 5.
Traffic exceeding the rate policy is dropped.
C. WWW traffic is limited to 10 Mb.
Conforming traffic is marked as IP precedence 5 and the next rate limit statement is executed.
Traffic exceeding the rate policy is dropped.
D. WWW traffic is limited to 20 Mb.
Conforming traffic is sent as IP precedence 5.
Traffic exceeding the rate policy is sent with best effort priority.
E. WWW traffic is limited to 20 Mb.
Conforming traffic is marked as IP precedence 5 and the next rate limit statement is executed.
Traffic exceeding the rate policy is sent with best effort priority.

Answer: D

Explanation:



The configuration implements the policy outlined in the previous case study. Traffic is classified with extended access lists (to differentiate web traffic from other traffic), and CAR uses the access list to apply the correct policing to the traffic.
Precedence values of 0 and 1 are set to signal preferential treatment of the webtraffic to other QoS mechanisms, such as queuing and WRED.
The access list 101 identifies HTTP traffic using the default well-known port number 80 ("www" in the configuration) either as the source or destination port number in TCP segments. The conforming part of the class (up to 512 kbps) is marked with IP precedence 1. The exceeding part of the class is further evaluated by the next rate-limit command where it is limited together with the rest of the traffic (non-HTTP) to 256 kbps. The total throughput, therefore, will never exceed 768 kbps (512 kbps of conforming HTTP traffic + 256 kbps of exceeding HTTP traffic and all other traffic). WRED can be used in combination with CAR to provide differentiated congestion avoidance anywhere in the network.
Source: Cisco IP QoS Traffic Shaping and Policing, Page 4-93

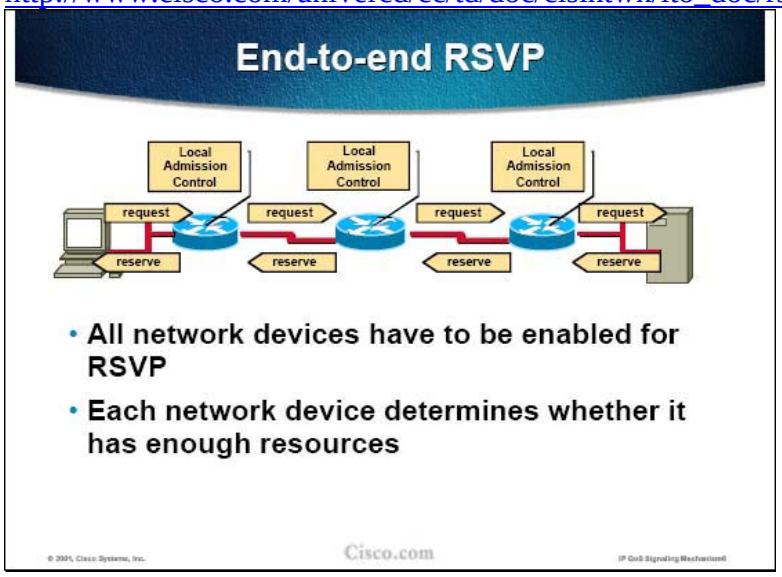
QUESTION 191
What are functions of the RSVP path message? (Choose all that apply.)

A. RSVP path message transports the path state to each node.
B. RSVP path message distributes the path table to each RSVP node in the network.
C. RSVP path message identifies the routes used for reservation-request messages in the reverse direction.
D. RSVP path message discovers all paths to the destination so that the best path can be chosen.

Answer: A, D

Explanation:
A: A path message is used to store the path state in each node.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm



If end-to-end RSVP is desired in a network, all devices in the reservation path must be RSVP-enabled. When a device receives an RSVP message, it determines whether it has enough resources to satisfy the reservation request at the local level.

There are two main RSVP messages used for signaling. When a reservation is needed, the sending client sends an RSVP PATH message into the network requesting a specific bandwidth to a specific destination (or multicast address, in the case of IP multicast application). The purpose of the PATH message is to discover all RSVP-enabled routers along the path from the sender to the receiver, and to create initial reservations. The PATH message is forwarded along the flow path and every intermediate RSVP-capable router adds its identification to the PATH message. When the receiving end-node receives the PATH message, it confirms the reservation by replying with an RSVP RESV message. The RESV message is forwarded back upstream towards the initial sender using the list of

RSVP-enabled routers generated by the PATH message. If the RESV message successfully arrives at the initial sender, each hop in the end-to-end connection has reserved the appropriate resources and an end-to-end reservation is established. If the appropriate resources are not available, the reservation is refused and the application must default to traditional, best effort communications.

RSVP keeps track of the soft state of reservations in routers. This soft state provides dynamic membership information, adapts to routing changes, and, as the number of flows increases, enables dynamic changes in reservations to meet those changing needs. RSVP reservations time out unless periodically refreshed by the communication endpoint, usually at 30-second intervals.

The benefits of soft state behavior are:

Connectionless behavior - routers automatically adapt to route changes.

Timeliness - state changes propagate immediately, but only as far as needed.

Robustness - the method is self-correcting, because incorrect reservations will always time-out even in the most unexpected situations.

Flexibility - provides easy dynamic reservation changes.
The cost of this approach is that it requires ongoing refresh processing for established states by the endpoints.
Sources: Cisco IP QoS Signaling Mechanism, Pages 7-4, 7-5

QUESTION 192
With Modular QoS CLI, which command should you use to display the configuration for the specified class of the specified policy map?

A. Show policy
B. Show policy-map class
C. Show policy-map service
D. Show policy-map interface

Answer: B

Explanation:
Reference:
http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1839/products_command_reference_chapter09186a008010

QUESTION 193
Which statement is true about policing traffic conditioners in IP QoS?

A. Policing records transmit queue to offer priority service to specific traffic flows.
B. Policing utilities buffers to delay excessive traffic when the flow is higher than expected.
C. Policing techniques monitor network traffic loads in an effort to anticipate and avoid congestion.
D. Policing allows network administrators to traffic engineer paths through the network for application flows.
E. Policing is the ability to control bursts and conform traffic to ensure certain traffic types receive specified amounts of bandwidth.

Answer: E

QUESTION 194
What are the two main functions of Committed Access Rate on Cisco IOS routers? (Choose two)

A. Packet classification using IP Precedence or QoS Group.
B. Bandwidth management by policing to control the maximum traffic rate.
C. Integrated services compatibility provided by an embedded RSVP signalling mechanism.
D. Integrated packet deliver de-jitter buffering mechanism to ensure real-time packet delivery.

Answer: A, B

Explanation:
CAR is a mechanism used to limit the traffic rate of a class and optionally mark packets with one of the following markers:
1) IP precedence
2) DSCP
3) MPLS experimental bits
4) QoS group
CAR can also mark packets with two different values depending on whether they:
1) Conform to the policy (packet is within the contractual bit-rate)
2) Exceed the policy (packet is over the contractual bit-rate)
Conforming and exceeding packets can be marked with different values.
Reference: Introduction to IP QoS p.2-47

QUESTION 195
What are two purposes of the RSVP patch message? (Choose two)

A. Transports the path state to each node.
B. Sets up an alternate path in case of network failure.
C. Distributes the path table to each RSVP node in the network.
D. Discovers all paths to the destination so that the best path can be chosen.
E. Identifies the routers used for reservation-request messages in the reverse direction.

Answer: A, D

Explanation:
A: A path message is used to store the path state in each node.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm

---

QUESTION 196
The "show ip rsvp" installed command displays what information?

A. RSVP-related interface information.
B. Current peak rate limit set for an interface.
C. RSVP neighbors installed in the adjacency table.
D. RSVP-related receiver information currently in the database.
E. RSVP-related installed filters and corresponding bandwidth information.

Answer: E

Explanation:
The show ip rsvp installed command shows all active conversations over an RSVP-enabled path, which has resource reservations installed. The actual reserved

bandwidth is shown, along with the session parameters (endpoints and applications).
Reference: Introduction to IP QoS p.7-18

QUESTION 197
When configuring Resource Reservation Protocol (RSVP), how much of the available RSVP bandwidth is available to a single flow if you do not explicitly specify an amount?

A. 25%
B. 50%
C. 75%
D. 100%

Answer: C

Explanation:
Basic RSVP is configured by two interface commands. The rsvp bandwidth command sets the maximum total amount of reservable bandwidth on an interface. By default, it is configured to 75% of the configured bandwidth, which is also its maximum allowed value. A per-flow reservable bandwidth can also be configured, setting the maximum bandwidth a single flow can reserve over this interface. By default, it is also set to 75% of the configured bandwidth.
Reference: Introduction to IP QoS p.7-9

QUESTION 198
Which two are important benefits of applying QoS to IP networks? (Choose two)

A. QoS manages packet loss during periods of bursty congestion.
B. QoS allows network managers to control usage patterns of network applications.
C. QoS can solve traffic problems on low bandwidth, high-latency, high-loss WAN links.
D. QoS facilities the integration of differing traffic types such as voice, video, and data into a single infrastructure.
E. QoS can provide performance enhancements for commercial application issues such as server sizing and tuning.

Answer: A, D

QUESTION 199
What could be the reasons why real-time applications such as VoIP require better service in which to operate than the traditional best-effort services? (Choose all that apply.)

A. These applications are jitter sensitive.
B. These applications are delay sensitive.
C. Real-time applications are sensitive to packet drops.
D. Real-time applications are usually non-interactive and use mostly bulk data transfer.
E. Real-time applications usually require RSVP which is not available on best-effort services.

Answer: A, B, C

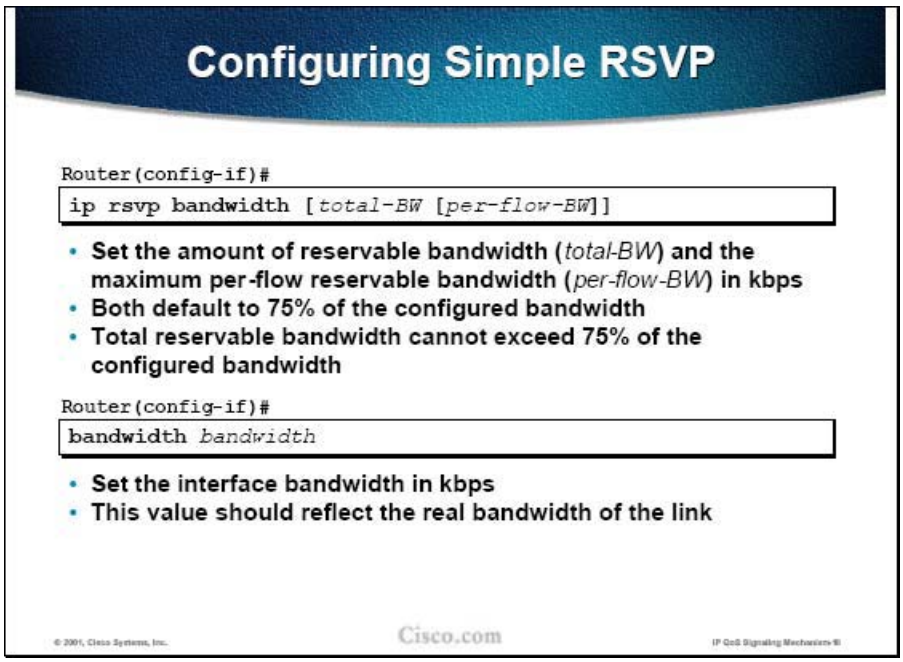
Explanation:
Quality of Service is usually identified by the following parameters:
Amount of bandwidth available to a certain application or user
Average delay experienced by IP packets on end-to-end or link basis
Jitter that affects applications that transmit packets at a certain fixed rate and expect to receive them at approximately the same rate (for example, voice and video)
Drops of packets when a link is congested can severely impact fragile applications
Admission control which prevents too many sessions from congesting links and causing degradation in quality of service (for example, voice sessions)
Source: Cisco IP QoS Introduction, Page 4

QUESTION 200
What is the default amount of interface bandwidth available to RSVP?

A. 10%
B. 25%
C. 50%
D. 75%
E. 100%

Answer: D

Explanation:



Basic RSVP is configured by two interface commands. The ip rsvp bandwidth command sets the maximum total amount of reservable bandwidth on an interface. By default, it is configured to 75% of the configured bandwidth, which is also its maximum allowed value. A per-flow reservable bandwidth can also be configured, setting the maximum bandwidth a single flow can reserve over this interface. By default, it is also set to 75% of the configured bandwidth.
Note RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).
The bandwidth interface command sets the interface bandwidth and is used by routing protocols (to calculate costs) and by a variety of QoS mechanisms. With RSVP, this is used as the configured bandwidth parameter, referenced by the limits in the ip rsvp bandwidth command.
Source: Cisco IP QoS Signaling Mechanism, Page 7-9

QUESTION 201
How is flow-based WFQ applied at the Virtual Circuit (VC) level?

A. Configure fair-queuing in the ATM VC.
B. Configure fair-queuing in the policy map.
C. Configure fair-queuing in the default class.
D. Configure fair-queuing in the service policy.

Answer: C

QUESTION 202
Exhibit:
class-map ixia
match input-interface FastEthernet3/0
class-map loopbacks

```
match access-group 102
!
policy-map mypol
class ixia
bandwidth 40000
queue-limit 40
class loopbacks
bandwidth 10000
class class-default
fair-queue
!
interface ATM2/0.130 point-to-point
ip address 14.0.0.2 255.0.0.0
no ip directed-broadcast
pvc 1/130
service-policy output mypol
vbr-nrt 100000 75000
broadcast
encapsulation aa15mux ip
!
access-list 102 permit ip host 10.0.0.1 host 11.0.0.1
```

Which four statements are true about the configuration in the exhibit? (Choose four)

A. CBWFQ is applied to PVC 1/130.
B. One class is applied to all the incoming traffic on Fast Ethernet 3/0.
C. Class loopbacks have been assigned a minimum of 10 kbps bandwidth
D. Class ixia has been allocated 40 Mbps bandwidth and a queue depth of 40 packets.
E. Flow-based WFQ is applied to all packets that do not belong to either class ixia or loopbacks.

Answer: A, B, D, E

QUESTION 203
How does RSVP-AT, QoS Interworking provide L3 QoS over ATM (L2)?

A. It builds an SVC with the desired parameters for each L3 flow.
B. It maps each L3 flow to a separate soft PVC that is configured with the appropriate parameters.
C. It dynamically builds a sub-interface for each flow and uses WFQ to achieve its bandwidth and latency requirements.
D. It dynamically allocates the L2 flow to an existing VC that can guarantee the bandwidth and latency requirements.

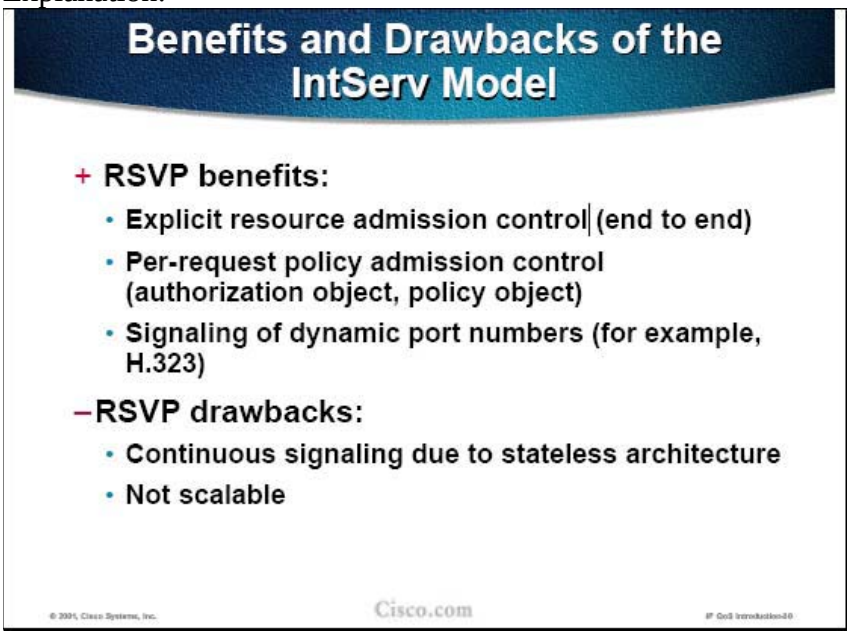
Answer: A

QUESTION 204
Why would you advice the new Certkiller trainee technician to make use of RSVP in an Integrated Services model? (Choose all that apply.)

A. Admission control can be based on per-request polices.
B. RSVP provides continues signaling due to its stateless architecture.
C. End-to-end, explicit resource admission control is possible with RSVP.
D. RSVP is very scalable, even in the backbone, as only a small amount of information is required for each RSVP flow.
E. RSVP provides signaling for dynamic port numbers such as those uses in H.323.

Answer: A, C, E

Explanation:



The main benefits of RSVP are:
It signals QoS requests per individual flow. The network can then provide guarantees to these individual flows. The problem of this is that it does not scale to large networks because of the large numbers of concurrent RSVP flows.
It informs network devices of flow parameters (IP addresses and port numbers). Some applications use dynamic port numbers, which can be difficult for network devices to recognize. NBAR is a mechanism that has been introduced to supplement RSVP for applications that use dynamic port numbers but do not use RSVP.
It supports admission control that allows a network to reject (or down-grade) new RSVP sessions if one of the interfaces in the path has reached the limit (all reservable bandwidth is booked).
The main drawbacks of RSVP are:
Continuous signaling due to stateless operation of RSVP
RSVP is not scalable to large networks where per-flow guarantees

would have to be made to thousands of flows.
Source: Cisco IP QoS Introduction, Page 30

QUESTION 205
The newly appointed Certkiller trainee technician wants to know what the function of classification as a building block of QoS in IP networks is. What will your reply be?

A. It is to recognize and distinguish different traffic streams.
B. It is to delay or drop packets based on specific traffic polices.
C. It is to provide guaranteed bandwidth to individual traffic streams.
D. It is to speed transmission and compress headers, improving WAN efficiency.

Answer: A

QUESTION 206
Study the Exhibit below carefully:
Policy-map shape-it
Class customer1
Bandwidth
Class customer2
Bandwidth 384
Interface serial 3
Service-policy output shape-it
You want to add CB shaping to interface serial 3, so that each customer is shaped to 64 Kbps beyond what is committed to the. Which command needs to be added to the policy map for customer 2?

A. shape average 448
B. shaping average 448
C. shape average 448000
D. shaping average 448000

Answer: C

QUESTION 207
Study the Configuration below carefully:
interface multilink 1
ip addr 1.1.1.1 255.0.0.0
fair-queue
ppp multilink
ppp multilink fragment-delay 140 160
Which statement will be valid for this configuration?

A. Fragmentation is not yet enabled.
B. Fragmentation is only partially enabled.

C. Fragmentation is enabled, but packets will not be interleaved.
D. Fragmentation is enabled, and voice packets or fragments, plus packets smaller than 140 bytes, will be interleaved.
E. Fragmentation is enabled, but only packets shorter than 160 bytes will be interleaved between fragments.

Answer: C

Explanation: The following command is not visible
ppp multilink interleave
Reference: http://www.cisco.com/en/US/products/sw/iosswrel

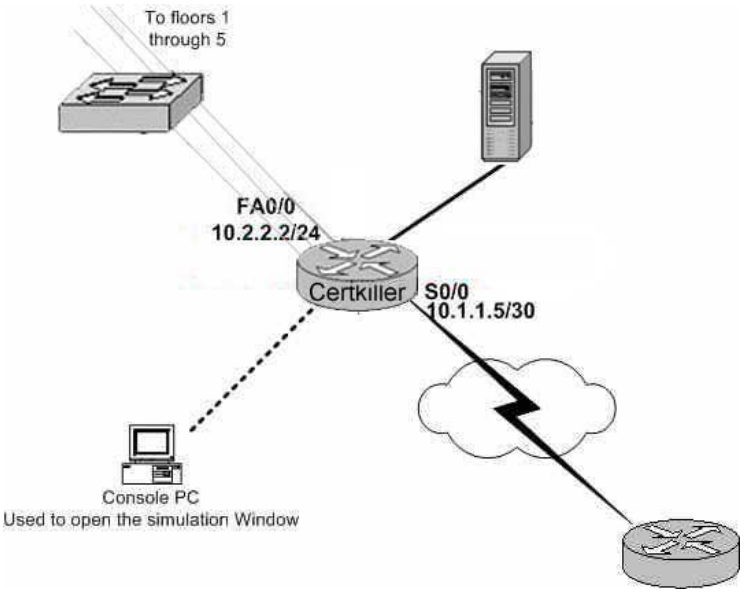
QUESTION 208
Which of the following statements describes Network-Based Application Recognition (NBAR)?

A. NBAR is Cisco IOS software that is capable of recognizing applications that use dynamically assigned port numbers or applied services (including QoS) to them.
B. NBAR is an application associated with RSVP that resides in the host computers and is responsible for registering its network applications with RSVP to allocate the necessary bandwidth for each.
C. NBAR is an application that is responsible for the search and cataloguing of applications in use on the network on the network servers. The latter can be used by the network administrator to apply services, including QoS.
D. NBAR is a network server that uses agents in the routers to monitor the network to catalog the application traffic and applied services, including QoS.

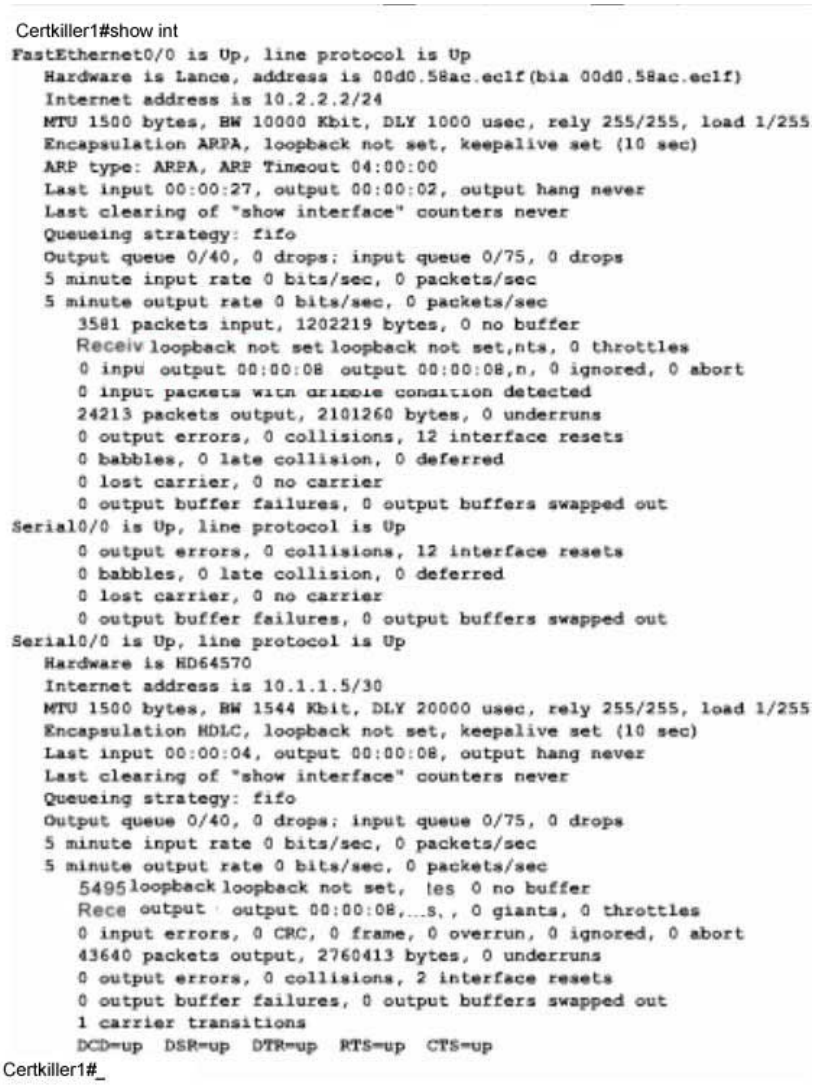
Answer: A

Explanation:
NBAR is a mechanism that has been introduced to supplement RSVP for applications that use dynamic port numbers but do not use RSVP.
Source: Cisco IP QoS Introduction, Page 30

QUESTION 209
SIMULATION
Network topology exhibit:



You work as an administrator for Certkiller .com. On the Certkiller 1 WAN edge router use Class-Based Marking to classify and mark the inbound traffic to FA0/0 from the Campus LAN as follows:
Create a policy-map called " Certkiller " with the following 3 classes.
Class Name Traffic Type PHB
real-time rtp voice packets EF
(Use NBAR to match the rtp voice packets.)
mission-critical citrix or voice control traffic AF31
(Use NBAR to match the citrix traffic.)
(For the voice control traffic reference the given
named access-list to use as the match criteria.)
bulk ftp traffic AF11
(Use NBAR to match the citrix traffic.)
class-default all others Default
Show int command output exhibit:

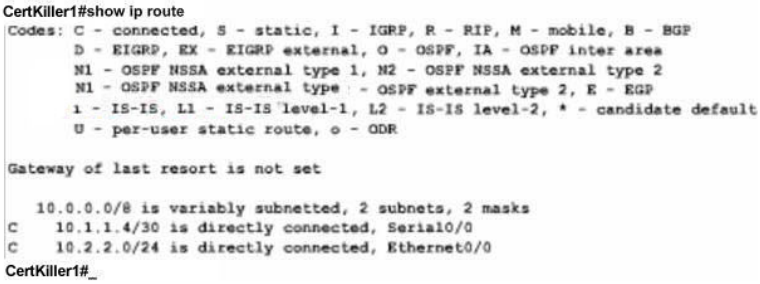


```
Certkiller1#show int
FastEthernet0/0 is Up, line protocol is Up
   Hardware is Lance, address is 00d0.58ac.ec1f(bia 00d0.58ac.ec1f)
   Internet address is 10.2.2.2/24
   MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
   Encapsulation ARPA, loopback not set, keepalive set (10 sec)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 00:00:27, output 00:00:02, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      3581 packets input, 1202219 bytes, 0 no buffer
      Receiv loopback not set loopback not set,nts, 0 throttles
      0 inpu output 00:00:08 output 00:00:08,n, 0 ignored, 0 abort
      0 input packets with dribble condition detected
      24213 packets output, 2101260 bytes, 0 underruns
      0 output errors, 0 collisions, 12 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
Serial0/0 is Up, line protocol is Up
      0 output errors, 0 collisions, 12 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
Serial0/0 is Up, line protocol is Up
   Hardware is HD64570
   Internet address is 10.1.1.5/30
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
   Encapsulation HDLC, loopback not set, keepalive set (10 sec)
   Last input 00:00:04, output 00:00:08, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      5495 loopback loopback not set, les 0 no buffer
      Rece output output 00:00:08,...s, , 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      43640 packets output, 2760413 bytes, 0 underruns
      0 output errors, 0 collisions, 2 interface resets
      0 output buffer failures, 0 output buffers swapped out
      1 carrier transitions
      DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
Certkiller1#_
```

Show runn command output exhibit:

```
Certkiller1#show runn
Building configuration...
Current configuration:
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
!
!
logging queue-limit 100
!
ip subnet-zero
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.2.2.2 255.255.255.0
 speed auto
 duplex auto
!
interface Serial0/0
 ip address 10.1.1.5 255.255.255.252
 bandwidth 384
!
!
ip http server
ip classless
!
!
!
ip access-list extended Voice-Control
remark - use to match the voice control traffic
permit tcp any any eq 1720
permit tcp any any range 11000 11999
permit udp any any eq 2427
permit udp any any eq 1728
permit udp any any eq ge 2000 2002
permit udp any any eq 1719
permit udp any any eq 5060
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
```

Show ip route output exhibit:



Answer:
Certkiller 1(config)#class-map real-time
Certkiller 1(config-cmap)#match protocol rtp voice
Certkiller 1(config-cmap)#class-map citrix-or-mission-critical
Certkiller 1(config-cmap)#match protocol citrix
Certkiller 1(config-cmap)#match access-group voice-control
Certkiller 1(config-cmap)#class-map bulk
Certkiller 1(config-cmap)#match protocol ftp
Certkiller 1(config-cmap)#class-map class-default
Certkiller 1(config-cmap)#match any
Certkiller 1(config)#policy-map test
Certkiller 1(config-pmap)#class real-time
Certkiller 1(config-pmap-c)#set ip dscp ef
Certkiller 1(config-pmap-c)#class bulk
Certkiller 1(config-pmap-c)#set ip dscp af11
Certkiller 1(config-pmap-c)#class citrix-or-mission-critical
Certkiller 1(config-pmap-c)#set ip dscp af31
Certkiller 1(config-pmap-c)#class class-default
Certkiller 1(config-pmap-c)#set ip dscp default
Certkiller 1(config)#interface fastethernet 0/0
Certkiller 1(config-if)#service policy input test
Certkiller 1(config-if)#end
Certkiller 1#copy run start
Note: There is no need to use the ip cef or ip nbar protocol-discovery commands as provided in older versions since the question doesn't state to configure NBAR.
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nbarw_wp.htm

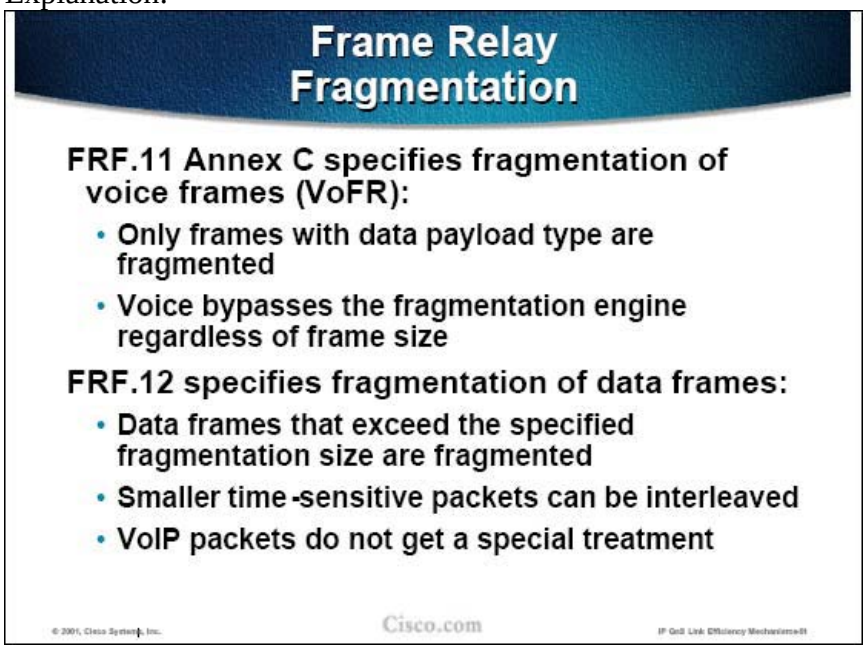
---

QUESTION 210
Which statement regarding Frame Relay Fragmentation is valid?

A. Voice packets are never fragmented.
B. FRF.12 uses separate queues for voice and non-voice traffic.
C. All DLCIs on the same physical interface must use the same fragmentation scheme.
D. FRF.11 Annex-C is used if VoFR is configured on the DLCI.
E. An interface uses FRF.11 Annex-C or FRF.12 fragmentation for non-voice traffic and FRF 3.1 encapsulation for voice traffic.

Answer: D

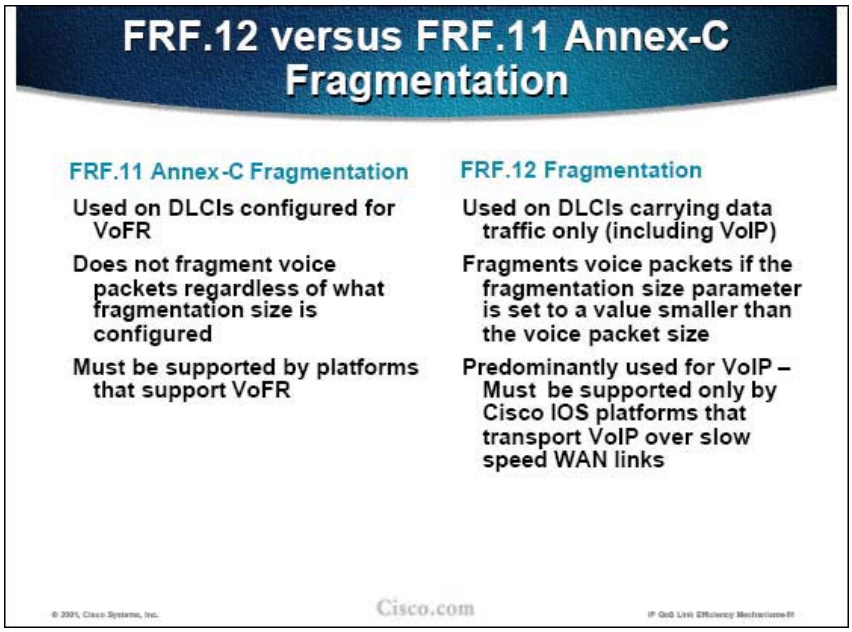
Explanation:



In Frame Relay networks, two fragmentation standards are available on layer-2 (within the Frame Relay encapsulation):

When Voice over Frame Relay (FRF.11) and fragmentation are both configured on a PVC, Frame Relay fragments are transmitted in the FRF.11 Annex C format. This fragmentation method is used when FRF.11 voice traffic is transmitted on the PVC and uses the FRF.11 Annex C fragmentation standard. With FRF.11, all data packets contain fragmentation headers regardless of size. This form of fragmentation is not recommended for use with Voice over IP.

FRF.12 fragmentation is defined by the FRF.12 Implementation Agreement. The FRF.12 Implementation Agreement was developed to allow long data frames to be fragmented into smaller pieces and interleaved with real-time frames. In this way, real-time voice and non-real-time data frames are carried together on lower-speed links without causing excessive delay to the real-time traffic. As a result, FRF.12 is the recommended fragmentation to be used with VoIP.



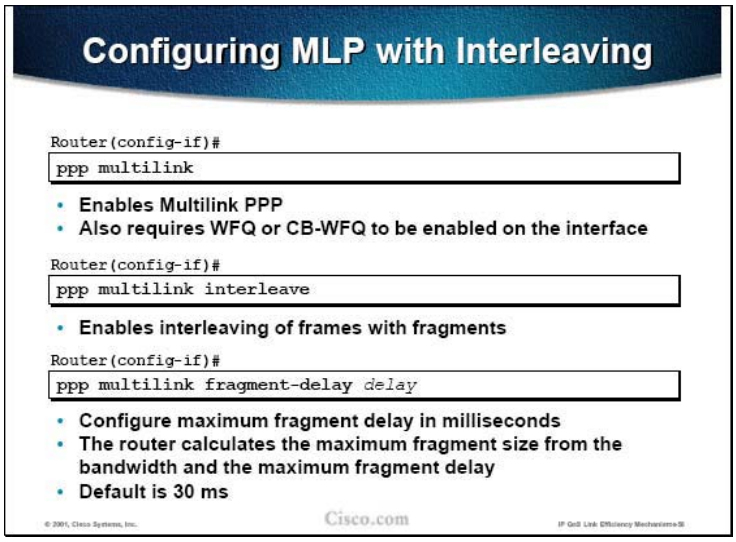
If a PVC is not configured for VoFR, it uses normal Frame Relay (FRF.3.1) data encapsulation. If fragmentation is turned on for this DLCI, it uses FRF.12 for the fragmentation headers. PVCs carrying VoIP use FRF.12 fragmentation because VoIP is a layer 3 technology that is transparent to layer 2 Frame Relay. VoIP and VoFR can be supported on different PVCs on the same interface, but not on the same PVC.
FRF.12 fragments voice packets if the fragmentation size parameter is set to a value smaller than the voice packet size. FRF.11 Annex-C (VoFR) does not fragment voice packets regardless of what fragmentation size is configured.
FRF.11 Annex-C needs only to be supported by platforms that support VoFR. Because FRF.12 is predominantly used for VoIP, it is important to use FRF.12 as a general feature on Cisco IOS platforms that transport VoIP over slow speed WAN links.
Sources: IP QoS Link Efficiency Mechanisms 6-53, 6-54

QUESTION 211
Which of the following represents the default MLP Link Fragmentation and Interleaving (LFI) serialization time?

A. 10 ms
B. 20 ms
C. 30 ms
D. 40 ms
E. 50 ms

Answer: C

Explanation:



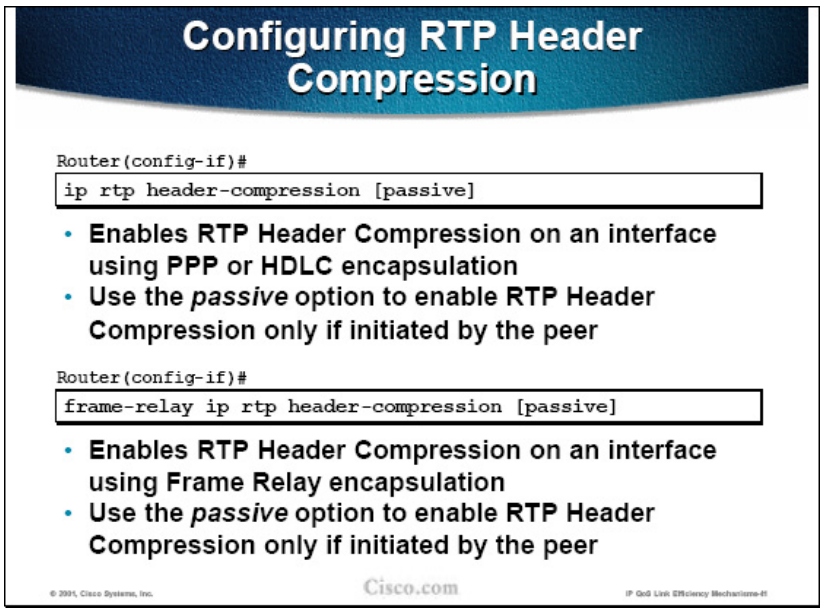
The ppp multilink command enables PPP multilink on an interface. This requires either Weighted Fair Queuing (WFQ) or CB-WFQ (Class-Based Weighted Fair Queuing) to be enabled on the same interface.
The ppp multilink interleave command enables interleaving of fragments within the multilink connection.
The ppp multilink fragment delay command specifies the maximum desired fragment delay for the interleaved multilink connection. The maximum fragment size is calculated from the interface bandwidth and the specified maximum delay. The default is set at 30 milliseconds.
If dCEF is configured on a VIP interface, MLP with interleaving runs distributed on the VIP.
Source: Cisco IP QoS Link Efficiency Mechanisms, Page 6-49

QUESTION 212
Which of the following functions does the passive keyword perform when configuring Compressed Real-time Transport Protocol (RTP)?

A. It compresses all RTP packets, regardless of other parameters.
B. It compresses all outgoing RTP packets; incoming RTP packets do not need to be.
C. It compresses outgoing RTP packets only if incoming RTP packets are compressed.
D. Incoming RTP packets may be compressed; all outgoing RTP packets are not compressed.

Answer: C

Explanation:



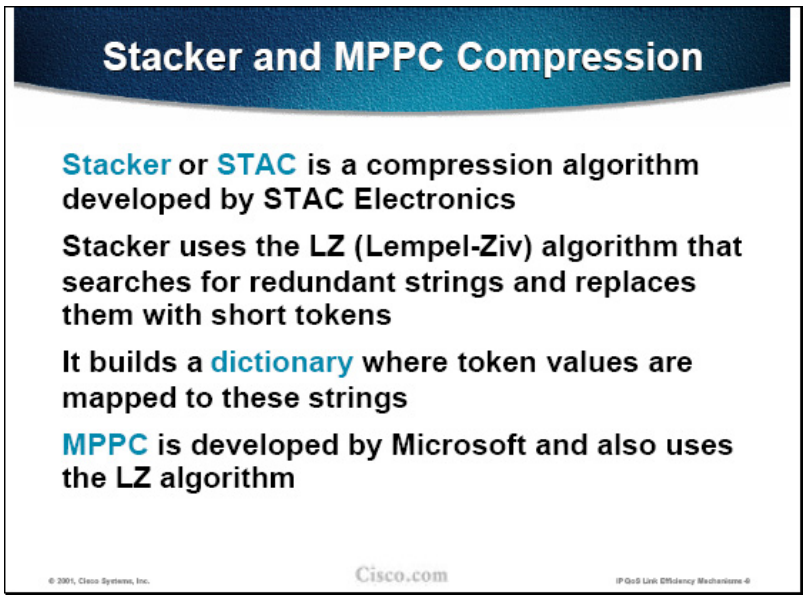
RTP header compression is configured with the ip rtp header-compression command. The passive option instructs the peer to use RTP header compression only if the remote peer initiates RTP header compression.
On frame relay, the frame-relay ip rtp header-compression configures header compression with interfaces using pure frame relay encapsulation.
In Cisco IOS, RTP header compression is now fast and CEF-switched. If distributed CEF (dCEF) is configured, CRTP also runs in distributed mode. Up to 256 connections, which is also the default value, can be compressed over a point-to-point link.
Source: Cisco IP QoS Link Efficiency Mechanisms, Page 6-36

QUESTION 213
The newly appointed Certkiller trainee technician wants to know which of the following Cisco IOS-supported payload compression algorithms will search the byte stream for redundant strings and replace them with shorter dictionary tokens. What will your reply be? (Choose all that apply.)

A. Diffie-Helman (DH)
B. Microsoft Point-to-Point Compression (MPPC)
C. Predictor
D. STAC (Stacker)

Answer: B, D

Explanation:



The STAC (or Stacker) algorithm is based on the well-known LZ (Lempel-Ziv) compression algorithm. The LZ (sometimes also called LZW) algorithm searches the byte stream for redundant strings, and replaces them with shorter dictionary tokens. The dictionary is built in real time, and there is no need to exchange the dictionary between the compression peers, because the dictionary is reconstructed from the data received by the remote peer. The MPPC method also uses the same LZ algorithm. The STAC and MPPC algorithms yield very good compression results, but are CPU-intensive.
Source: Cisco IP QoS Link Efficiency Mechanisms, Page 6-7

QUESTION 214
What is the standard serialization delay goal to ensure low delay and jilter for voice packets?

A. 20-25ms
B. 10-15ms
C. 15-20ms
D. 25-30ms

Answer: B
Reference: "Ip Telephony Self-Study / Cisco Ip Telephony Flash Cards", page. 167.

QUESTION 215
On a Cisco switch, CDP v2 must be enabled for which AutoQoS configuration to function properly?

A. WTT queuing
B. trust boundary
C. fr-atm
D. ciscosoflphone

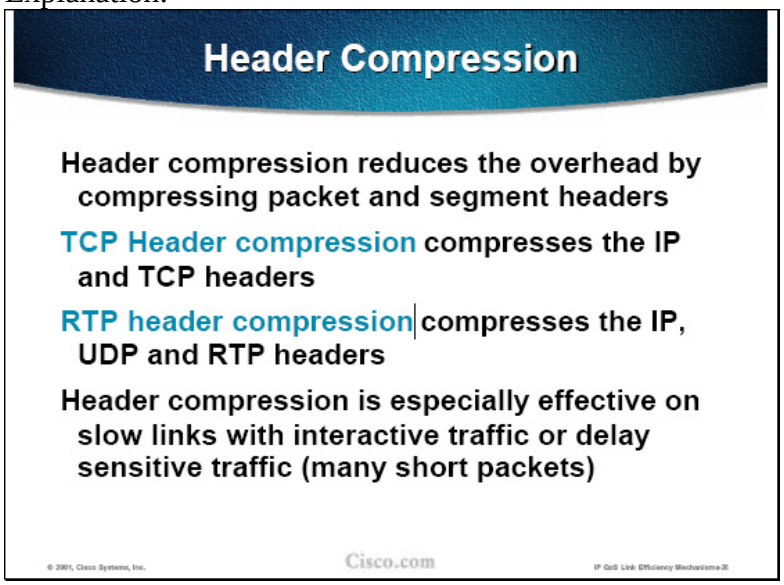
Answer: B

QUESTION 216
Which of the following headers can be reduces by making use of RTP header compression? (Choose all that apply.)

A. IP
B. TCP
C. UDP
D. RTP
E. PPP

Answer: A, C, D

Explanation:



All compression methods are based on eliminating redundancy when sending the same or similar data over a transmission medium. One piece of data, which is often repeated, is the protocol header. In a flow, the header information of packets in the same flow does not change much over the lifetime of that flow. Therefore, most of header information could be sent only at the beginning of the session, stored in a dictionary, and then referenced in later packets by a short dictionary index.
Two methods were standardized by the IETF (Internet Engineering Task Force) for use with IP protocols:
TCP header compression (also known as the Van Jacobson or VJ header compression) is used to compress the packet TCP headers over slow links, thus considerably improving the interactive application performance.
RTP header compression is used to compress UDP and RTP headers, thus lowering the delay for transporting real-time data, such as voice and video over slower links.
Source: Cisco IP QoS Link Efficiency Mechanisms, Page 6-21

QUESTION 217
Which statement regarding the policing traffic conditions in IP QoS is valid?

A. Policing allows the network administrators to traffic engineer paths through the network for application flows.
B. Policing techniques monitor network traffic loads to anticipate and avoid congestion.
C. Policing is the ability to control bursts and conform traffic to ensure certain traffic types receive specified amounts of bandwidth.
D. Policing reorders transmit queues to offer priority service to specific traffic flows.
E. Policing utilizes buffers to delay excessive traffic when the flow is higher than expected.

Answer: B
Incorrect:
C. With shaping, traffic bursts are smoothed out producing a steadier flow of data
E. Policing does not introduce any delay to traffic that conforms to traffic policies

Explanation:
The QoS tool used to monitor the rate, and discard the excess traffic, is called traffic policing, or just policing. Because the provider is monitoring traffic sent by the customer, traffic polices typically monitor ingress traffic, although they can monitor egress traffic as well.
Source: Cisco DQOS Exam Certification Guide, Page 95

QUESTION 218
When working in a large network which of the following would qualify to be a limiting factor of IntServ scalability?

A. IntServ admission control must be implemented locally on all the routers.
B. MPLS/TE tunnels cannot be established through an MPLS network using RSVP.
C. IntServ requires routers that are able to track a large amount of per-flow state information.
D. IntServ requires all routers that have the ability to identify common flows that require the same service into a traffic aggregate.
E. The IntServ QoS mechanism used to apply the appropriate per-hop behavior (PHB) must be implemented on all the routers.

Answer: C

Explanation:
Benefits and Drawbacks of the IntServ Model
Benefits and Drawbacks of the
The main drawbacks of RSVP are:
Continuous signaling due to stateless operation of RSVP.
RSVP is not scalable to large networks where per-flow guarantees

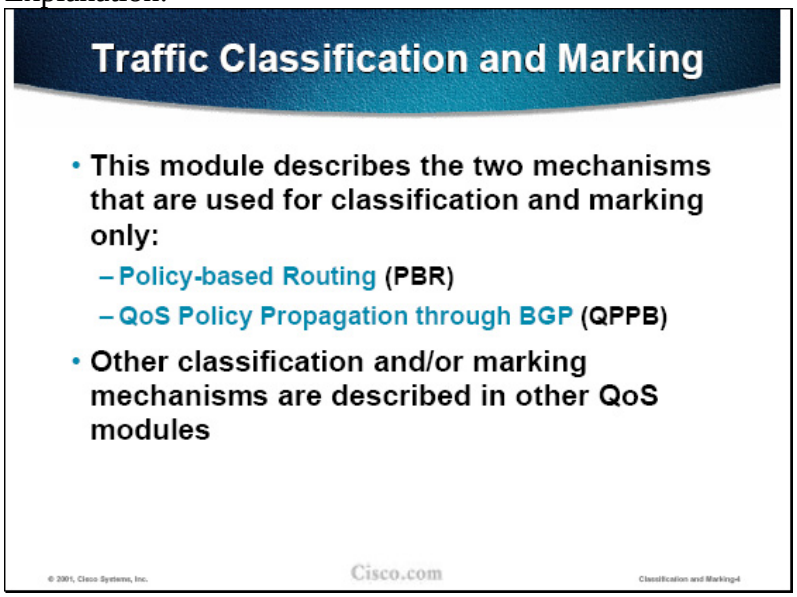
would have
to be made to thousands of flows.
Source: Cisco IP QoS Introduction, Page 30

QUESTION 219
What are the Cisco IOS QoS mechanisms that have marking abilities? (Choose all that apply.)

A. PBR
B. Committed Access Rate (CAR)
C. Weighted Random Early Detection (WRED)
D. QoS Policy Propagation through BGP (QPPB)
E. Class-Based Weighted Fair Queuing (CBWFQ)

Answer: A, B, D

Explanation:



This module describes the two QoS mechanisms that are used purely for classification and marking purposes:
Policy-based Routing (PBR)
QoS Policy Propagation through BGP (QPPB)
There are other QoS mechanisms that also support classification and marking:
Committed Access Rate (CAR) - this mechanism is described in the "IP QoS - Traffic Shaping and Policing" module
Class-based Policing (CB-Policing) - this mechanism is described in the "IP QoS - Modular QoS CLI (Chapter 2)" module
Class-based Marking (CB-Marking) - this mechanism is described in the "IP QoS - Modular QoS CLI (Chapter 2)" module
Source: Cisco IP QoS Classification and Marking, Page 2-3

QUESTION 220
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know which of the following is a "Measurement Based" Call Admission Control (CAC) function. What will your reply be?

A. RSVP
B. Advanced Busy Out Monitor (AVBO)
C. Service Assurance Agent (SAA)
D. Max. Connections
E. Voice Bandwidth for Frame Relay

Answer: B

Explanation:
Advanced Busy-Out Monitor (AVBO) is measurement based CAC feature.
Probe measurements are better than a configured "impairment factor"; if value is higher, the entire trunk is placed in busy-out.
Reference: DQOS Exam Certification Guide p.102

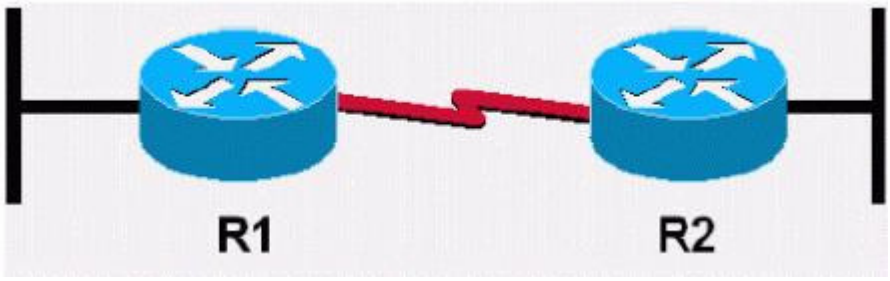
QUESTION 221
Which of the following represents a "Local Configuration" Call Admission Control (CAC) method?

A. RSVP
B. PSTN Fallback
C. Max. Connections
D. Locations Construct
E. Advanced Busy Out Monitor (AVBO)

Answer: C

Explanation:
Max-connections is Local based CAC tool. A configured number of maximum connections on the dial peer used for the call has been exceeded.
Reference: DQOS Exam Certification Guide p.102

QUESTION 222
Exhibit:



You want to apply policing and shaping functions to packets flowing into router1 over

Ethernet, over a serial link to router2, and onto another Ethernet to the destination host. Which statement is most accurate when describing Cisco's suggested design for policing and shaping?

A. Shaping is applied as output on router1's serial interface, and policing is applied on input of router2's serial interface.
B. Policing is applied as output on router1's serial interface, and shaping is applied on input of router2's serial interface.
C. Shaping is applied as output on router1's serial interface, and policing is applied on output of router2's Ethernet interface.
D. Policing is applied as output on router1's serial interface, and shaping is applied on output of router2's Ethernet interface.

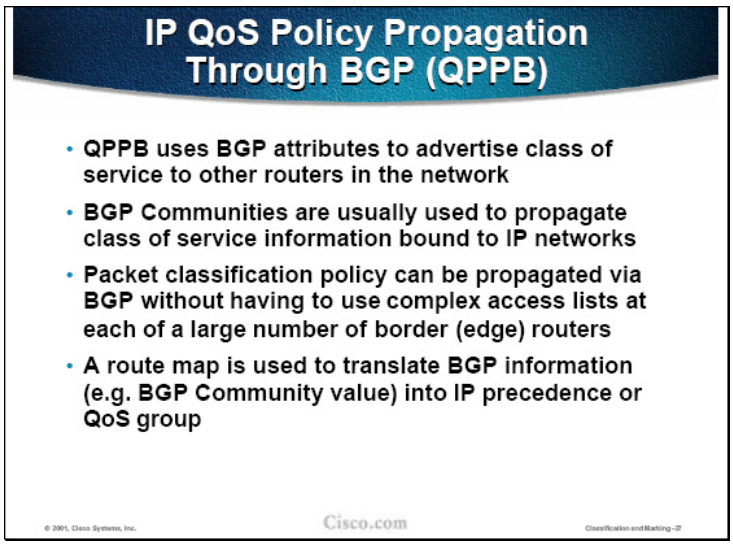
Answer: A

QUESTION 223
The newly appointed Certkiller trainee technician wants to know what is the purpose of the Cisco IOS Policy Propagation through BGP (QPPB) feature. What will your reply be?

A. QPPB enables traffic shaping on BGP-enable WAN interfaces.
B. It makes allowance for non-CEF enabled routers to support QoS and BGP by tagging routes in the BGP table.
C. It makes provision for flow-based Weighted Random Early Detection (WRED) support to external BGP peers.
D. It propagates IP precedence or the QoS Group to destinations using BGP communities.
E. It is responsible for providing QoS policy in BGP networks by allowing centralized QoS configurations in BGP confederations.

Answer: D

Explanation:



QoS Policy Propagation through BGP is a mechanism that can be split into two parts:

Policy propagation via BGP - where a QoS policy is encoded into a BGP attribute. BGP Communities are typically used to encode a QoS policy.

Marking of packets with IP precedence or QoS group based on the QoS policy learned via BGP.

BGP Policy is usually set on ingress routers (ingress for route propagation, egress for packet forwarding) in an Autonomous System. BGP then carries the information to other routers in the AS and translates (using a route map) this information into IP precedence or QoS group. Marking is then enabled on perinterface basis.

Source: Cisco IP QoS Classification and Marking, Page 2-23

QUESTION 224

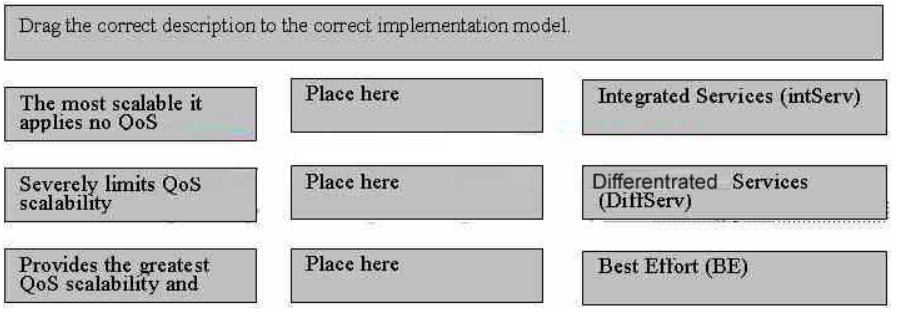
When is it recommended to use peak rate shaping over average rate shaping? (Choose two.)

A. when the network has additional bandwidth available beyond the CIR
B. when occasional packet loss can be tolerated by the application
C. when unlimited burst capability is required
D. when using class-based traffic shaping combination with CBWFQ
E. when using dual token bucket with class-based traffic shaping

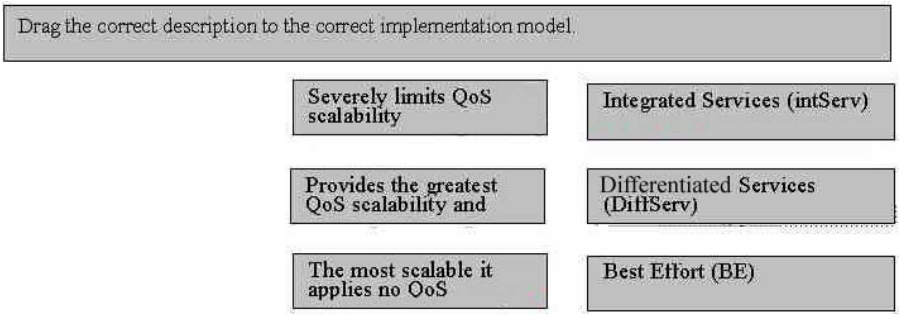
Answer: A, B

QUESTION 225

DRAG DROP



Answer:



QUESTION 226
What are three methods of reducing delay for critical applications in a converged network? (Choose three.)

A. Apply payload compression.
B. Increase link capacities.
C. Apply header compression.
D. Increase LF1 fragment size.
E. Reduce inter-packet gaps.
F. Increase all queue depths.

Answer: A, B, C

QUESTION 227
When configuring CB-WRED, on what is the default configuration based? (Choose two.)

A. IP precedence using 64 default WRED profiles
B. DSCP using 8 default WRED profiles
C. IP precedence using 8 default WRED profiles
D. treating non-IP traffic as precedence 0
E. treating non-IP traffic as DCSP Best Effort (BE)

Answer: C, D

QUESTION 228
If a priority queue is desired on a Cisco Catalyst 2950 switch, how can it be obtained?

A. A fifth priority queue is added
B. The fourth queue becomes the priority queue
C. Queues three and four are combined into one priority queue
D. Priority queuing is not supported on the Catalyst 2950

Answer: B
Cisco IP Telephony Flash Cards,
http//www.informit.com/articles/article.asp?p=352991&seqNum=7

QUESTION 229
Which technology is required when configuring FRF.12 on a Cisco device?

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

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

QUESTION 230
What are two differences between "shape average" and "shape peak" when configuring CB-Shaping (Choose two.)

A. Shape Average forwards Bc of traffic at every Tc interval with bursting capability
B. Shape average forwards Bc + Be of traffic at every Tc interval
C. Shape peak forwards Bc of traffic at every Tc interval with bursting capability
D. Shape peak forwards Bc + Be of traffic at every Tc interval
E. Share average uses a single or dual token bucket
F. Shape peak uses dual token bucket

Answer: A, D
Page 358, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 231
In LLQ, how does the command priority percent [i]percentage[/i] apply bandwidth to the priorty class?

A. There is no such command.
B. This class subcommand enables LLQ in this class, reserves bandwidth, and enables the policing function

Answer: B
Reference:
Page 290, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 232
Which TCP congestion control mechanism allows starvation and global synchronization to occur?

A. ECN
B. MDDR
C. RED
D. tail drop
E. WRR

Answer: D
Page 432, IP Telephony Self-Study Cisco DQOS Exam Certification Guide,
http//www.ciscopress.com/title/1587200589

QUESTION 233
What is the concept behind the operation of the Integrated Services model?

A. Application of network policies is only performed at the edges of the network.
B. Applications send as much data, with no predefined frequency, into the network.
C. Applications request a specific kind of service from the network and receive confirmation about reserved bandwidth and delay requirements before sending any data.
D. Applications are provided with a minimum amount of guaranteed bandwidth during periods of network congestion.
In periods of non-congestion, application can utilize all available bandwidth.
E. Network administrators predefine traffic classes for each application.
As application data traverse the network, packets are inspected and the network attempts to deliver the QoS level specified within the packet.

Answer: C

Explanation:
Integrated Services model is introduced to supplement the best-effort delivery by setting aside some bandwidth for applications that require bandwidth and delay guarantees. The Integrated Services model expects applications to signal their requirements to the network. Resource Reservation Protocol (RSVP) is used to signal QoS requirements to the network.
Reference: Introduction to IP QoS p.18

QUESTION 234
Which mechanism is used by IP RTP Priority to classify packets?

A. QoS Group
B. IP Precedence
C. Access Control List (ACL)
D. Differentiated Services Code Point (DSCP)
E. Dynamically Negotiated UDP ports within a specified range.

Answer: E

Explanation:
IP RTP Prioritization classifies packets based on UDP port numbers. If the destination UDP port is within the configured range it is enqueued into the high priority queue.
Reference: introduction to IP QoS p.3-136

QUESTION 235
What differentiates Modified Deficit Round Robin (MDRR) from Deficit Round Robin (DDR)?

A. In DDR, users can define multiple weights per queue.
B. MDRR designated one of its queues as a low-latency queue.
C. MDRR extends the number of queues supported from 8 to 32 queues.
D. DRR can facilitate guaranteed packet deliver through the use of Tx queue buffer and congestion feedback mechanisms.
E. Servicing of DDR queues is performed using a round robin weighted strategy, but in MDRR servicing is done using a FIFO strategy.

Answer: B

Explanation:
Modified Deficit Round-robin (MDRR) is a class-oriented queuing mechanism available on Cisco 12000 series routers (GSR).
It supports eight classes, one of which can be used for low-delay propagation.
DRR was the first implementation that was later improved by allowing one queue to be high priority.
Reference: Introduction to IP QoS p.3-18

QUESTION 236
The QoS pre-classify feature is used to ensure QoS services operate in conjunction with which two networking technologies? (Choose two)

A. VoIP
B. tunneling
C. Frame Relay
D. IPsec tunnel mode
E. multicast

Answer: B, D

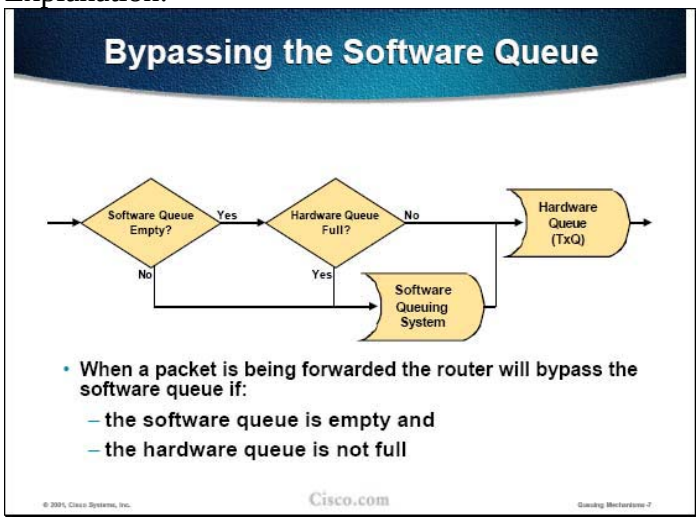
Explanation:
For Layer 2 Forwarding(L2F) and Layer 2 Tunneling Protocol(L2TP) protocols, the qos pre-classify command is applied on the virtual template interface. L2TP clients belonging to identical virtual private dial-up network (VPDN) groups inherit the preclassification setting. The qos pre-classify command can be configured on a per-VPDN tunnel basis.
For IPSec tunnels, the qos pre-classify command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00

QUESTION 237
When will packets be en-queued in the software queue?

A. when the shaping queue is full
B. when the hardware transmit queue is full
C. when the transmit ring reaches the congestion-discard threshold
D. when an incoming packet is process switched
E. when the egress trafic rate excees the ingress traffic rate
F. when an incoming packet is CEF switch

Answer: B

Explanation:



The implementation of software queuing was optimized for periods when the interface is not congested. The software queuing system is bypassed whenever there is no packet in the software queue and there is room in the hardware queue.
The software queue is, therefore, only used when data must wait to be placed into the hardware queue.
Source: Cisco Queuing Mechanisms, Page 3-6

QUESTION 238
Which of the following qualifies to be capabilities of CB shaping? (Choose all that apply.)

A. When it is similar to CAR with added shaping capabilities.
B. When it can be applied only as an output but not input shaper.
C. When it can be configured using MQC
D. When it is dissimilar to CAR with no additional shaping capabilities.
E. When it can be applied to individual VCs on a multipoint Frame Relay interface.

Answer: B, C

Explanation:
Class-based Shaping, like Class-based Policing, is used to rate-limit traffic within the CB-WFQ queueing system. Class-based Shaping works by metering the traffic rate and delaying excessive packets until they conform to the configured shaped rate.
Class-based Shaping is very similar to Generic Traffic Shaping (GTS), but is implemented as a part of the CB-WFQ system and is configured via the Cisco IOS MQC.
Like GTS, Class-based Shaping has no packet marking capability.
Reference: Introduction to IP QoS p.9-93

QUESTION 239
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know which three are primary functions of QPM. What will your reply be? (Choose all that apply.)

A. It can enable protocol discovery using NBAR
B. It can verify consistency of deployed QoS policies
C. It allows centralized enterprise-wide QoS policy
D. It combines configuration and monitoring into one tool
E. It scales QoS policy deployment quickly and accurately
F. All of the above.

Answer: B, C, E
Reference: DQOS Exam Certification Guide p.102

QUESTION 240
Under which circumstances will you use QPM? (Choose all that apply.)

A. When monitoring queue depth.
B. When ensuring end to end QOS commitments.
C. When measuring client response time.
D. When defining rules that match business requirements
E. When creating and deploying a decentralized enterprise-wide QOS policy.

Answer: B, D

Explanation:
You can use the Cisco QoS Policy Manager (QPM) to overcome the configuration correctness and consistency problem. QPM creates the QoS configurations for you, based on your input about QoS policies using a GUI. QPM loads the configurations, and re-verifies the QoS configurations to discover whether changes have been made. It can also reconfigure a router after someone has inadvertenly changed the QoS configuration - automatically. Any large QoS implementation begs for the use of QPM.

QUESTION 241
QDM Performance Monitor will graph which of the following metrics? (Choose all that apply.)

A. Drop Rate.
B. Packet Collisions and FCS error rates.
C. Pre/Post Policy Bit rate / Byte count /Packet Count.
D. Queue Depth.
E. Round trip packet delay.
F. All of the above.

Answer: A, C, D

Explanation:
The QDM user can perform two types of tasks. First, the user can configure QoS tools using a graphical interface from a browser. The user can also monitor real-time statistics about QoS behavior inside the single device, including graphs of bit/byte/packets rates, drop rates, queue depth, and so on.
Reference: DQOS Exam Certification Guide p.660

QUESTION 242
Which of the following show commands will display information regarding frame-relay fragmentation?

A. Show frame-relay pvc
B. Show frame-relay queue
C. Show frame-relay fragment
D. Show frame-relay tracert
E. Show frame-relay traffic shaping

Answer: C

Explanation:
The show frame-relay fragment command displays statistics of Frame Relay fragmentation methods. This output shows whether Frame Relay fragmentation is in effect and working as configured. The ouput also shows possible fragmentation timeouts, indicating that some fragments were lost in the Frame Relay network and could not be

reassembled. If the number of timeouts is significant, this may indicate significant frame loss in the Frame Relay network.
Reference: Introduction to IP QoS p.6-62

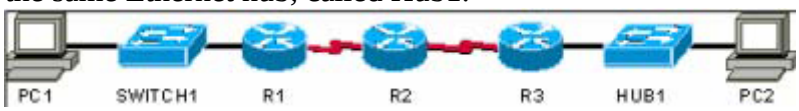
QUESTION 243
Which of the following statements would be the most appropriate when one considers Policy-Based Routing (PBR) for QoS?

A. PBR can only choose a route other than what is in the routing table.
B. PBR can change the route provided it first classifies and marks the packet.
C. PBR can change the route and/or mark the packet using precedence.
D. PBR can only set the precedence if configured to choose a route other than what is in the routing table.

Answer: C

Explanation:
The primary function of Policy-based Routing (PBR) is to bypass the destination-based forwarding functionality of routers by using a route map to make a forwarding decision based on other information.
One additional feature of Policy Based Routing is the ability to modify IP packets by marking them with IP precedence or QoS group.
Reference: Introduction to IP QoS p.2-5

QUESTION 244
The Exhibit below illustrates how an Ethernet frame is sent. PC1 will send an Ethernet frame, that is received and forwarded by Switch1. Switch1 forwards the frame to Router1. Router1 also forwards the packet to Router2 via serial link. Router2 will then forward the frame to Router3 via serial link, after which Router3 will forward the packet to the destination, PC2. Router3 and PC2 are connected to the same Ethernet hub, called Hub1.



Which networking devices can be used to examine the QoS field?

A. all devices
B. all routers
C. the hub and switches
D. all devices except the hub
E. Switch1 only
F. Switch1 and Router1

Answer: D

QUESTION 245
Which of the following statements regarding the capabilities of CB policing is valid?

(Choose all that apply.)

A. It cannot set ATM CLP bit.
B. It only allows conform, exceed or violate action.
C. It can be applied as either an input or output policer but not both.
D. It can be applied to serial as well as ATM and Frame Relay interfaces.
E. It can be applied as a cascading rate policy
F. It allows cascading rate policies, in order to allow for more granular rate limits.

Answer: B. D

Explanation:
B: is correct
Class-based policing can mark packets with three different values depending on whether they conform, exceed or violate the policy.
Reference: Introduction to IP QoS (Course) p.2-48

QUESTION 246
Study the Exhibit below carefully:

Exhibit 5

```
map-class frame-relay slow_vcs
  frame-relay traffic-rate 64000 2000
map-class frame-relay fast_vcs
  frame-relay traffic-rate 8000 4000


interface serial 0
no ip address
encapsulation frame-relay
frame-relay traffic-shaping
int s 0.2
  ip addr 1.1.1.1 255.0.0.0
  frame-relay interface-dlci 102
  class fast_vcs
int s 0.3
  ip addr 2.2.2.2 255.0.0.0
  frame-relay interface-dlci 103
  frame-relay class slow_vcs


interface serial 1
no ip address
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay class slow_vcs
int s 1.2
  ip addr 3.3.3.3 255.0.0.0
  frame-relay interface-dlci 202
int s 1.3
  ip addr 4.4.4.4 255.0.0.0
  frame-relay interface-dlci 203
```

Which interface or subinterface would be properly configured for 64 Kbps shaping?

A. interface S0
B. interface S1
C. subinterface S0.2
D. subinterface S0.3

E. subinterface S1.2

Answer: D

QUESTION 247
Which of the following are IPM features? (Choose all that apply)

A. identification and performance analysis
B. policy implementation right through an "IP reachable" network
C. Path Per Hop Performance Analysis between two network devices
D. real-time historical graphical reports
E. Proactive notification with an SNMP trap when response time exceeds predefined thresholds
F. All of the above

Answer: A, C, D, E

Explanation:
IPM can analyze the performance between two endpoints in the network by comparing probes generated and sent from different points in the network. Instead of just knowing that response time is slow, IPM can help pinpoint the slow point in the network. IPM also supports some historical reporting, although SMS has more historical reporting features. More importantly, you can set thresholds with IPM so that when network performance degrades past a certain point, it will generate an SNMP trap.
Reference: DQOS Exam Certification Guide p.666

QUESTION 248
You are the network administrator at Certkiller . The newly appointed Certkiller trainee wants to know which dial-peer subcommand correctly performs marking of VoIP packets. What will your response be?

A. precedence 5
B. ip precedence 5
C. set ip mark precedence 5
D. set ip precedence 5
E. mark ip precedence 5

Answer: B

Explanation:
The syntax of B is correct.
IP precedence is encoded into the three high-order bits of the ToS field in the IP header. It supports eight classes of which two are reserved and should not be used value and is usally used for the best-effort class. The set ip precedence command marks packets of a class with the specified precedence value.
Reference: Introduction to IP QoS p. 9-104

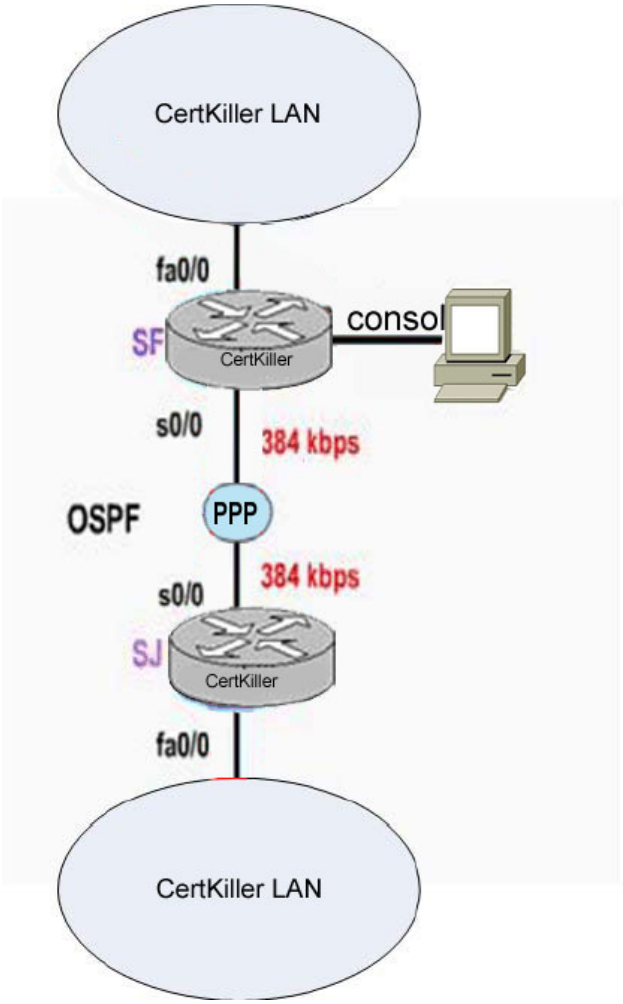
QUESTION 249
Under which circumstances will you use marking in QoS enabled networks?

A. When you want to indicate policing preferences based on the marked value.
B. When you want to color a packet or frame so it is distinguishable from other packets or frames in QoS treatment.
C. When you want to indicate whether PQ or CQ should be used.
D. When you want to enable a router to disregard its locally configured QoS settings and provide alternate QoS implied by the marked value.

Answer: B

Topic 1: Certkiller .com, Scenario

You work as a network administrator at the Certkiller .com main office in Las Vegas.
Study the Certkiller .com network topology exhibit carefully.
Exhibit:



Topic 1: Certkiller .com, (4 Questions)

QUESTION 250
For scenario refer to iPAD document.
The show ip nbar protocol-discovery command is entered on the SF router but no NBAR statistics outputs are being displayed.
What could solve this problem?

A. Configure the ip nbar protocol-discovery command within the fa0/0 interface configuration mode
B. Configure the ip nbar protocol-discovery command within the test-in policy-map configuration mode
C. Configure the ip nbar port-map command within the global configuration mode
D. Configure the ip nbar pdilm command within the global configuration mode
E. Configure the auto qos voip command within the S0/0 interface configuration mode

Answer: A

QUESTION 251
For scenario refer to iPAD document.
The SF and SJ routers are running protocol. Since a policy-map was applied to the SF router S0/0 interface, The SF and SJ routers are no longer able to establish full OSPF adjacency between them. Based on the DF router configuration and various show outputs from the SF router, which change to the policy-map in the SF router configuration could solve OSPF problem?

A. Change bandwith percent 5 for the Cs6 traffic class to bandwidth percent 25
B. Change bandwith percent 5 for the Cs6 traffic class to priority 8
C. Provide bandwidth guarantee to the class-default traffic class using bandwith percent 5
D. Use the no police 8000 conform-action drop exceed-action transmit command for the cs6 traffic class

Answer: D

QUESTION 252
For scenario refer to iPAD document.
Which statement is correct about the peer-to-peer traffic (Napster and Kazaa2) going out on the interface S0/0 on the SF router?

A. The peer-to-peer traffic will be classified into the p2p traffic class
B. The peer-to-peer traffic will be classified into the class default traffic class
C. The peer-to-peer traffic is not classified by the policy-map test, therefore all peer-to-peer traffic will be dropped.
D. The peer-to-peer traffic will have a maximum bandwidth guarantee of 25 percent of the S0/0 link bandwidth.
E. The peer-to-peer traffic will be policed to 8000 bps

Answer: B

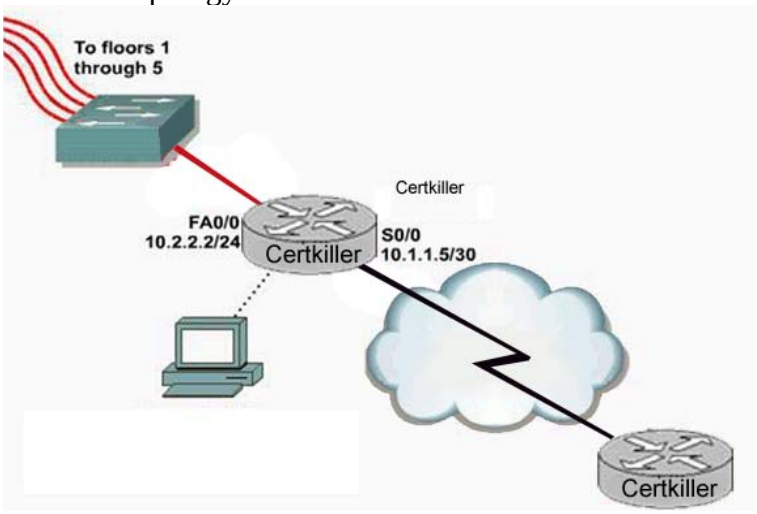
QUESTION 253
For scenario refer to iPAD document.
Which type of traffic will be policed to 5-Mbps ingress to the SF route fa0/0 interface?

A. All traffic matched by the ospf, bulk, Cs6, p2p, or interactive class-maps
B. All traffic matched by the bulk, Cs6, or interactive class-maps
C. All traffic not matched by the ospf, bulk, Cs6, p2p, or interactive class-maps
D. All traffic not matched by the bulk, Cs6, or interactive class-maps
E. All traffic

Answer: E

Topic 2: Certkiller .com Spain, Scenario

You work as a network engineer at the Certkiller .com satellite office in Madrid.
Network topology exhibit:



Topic 2: Certkiller .com Spain, (5 Questions)

QUESTION 254
For scenario refer to iPAD document.
What will happen if the incoming mission-critical traffic rate arriving at the fA0/0 interface is higher than the normal burst rate (CIR) but not exceeding the excess burst rate?

A. Dropped
B. Marked as AF31 then transmitted
C. Marked as AF32 then transmitted
D. Marked as AF33 then transmitted
E. Queued in the CBWFQ

Answer: C

QUESTION 255
For scenario refer to iPAD document.
What will happen if the incoming bulk class traffic rate arriving at the fa0/0 interface is higher than the normal burst rate (CIR)?

A. Dropped
B. Marked as DSCP 0 then transmitted
C. Queued in the excess token bucket
D. Queued in the CBWFQ

Answer: A

QUESTION 256
For scenario refer to iPAD document.
All traffic belonging to the class-default traffic class on the s0/0 interface will be queued by a class queue that uses which type of queuing?

A. FIFO
B. LLQ
C. WFQ
D. Round Robin
E. PQ

Answer: A

QUESTION 257
For scenario refer to iPAD document.
Which type of software queue is used on the s0/0 interface?

A. FIFO
B. CBWFQ
C. LLQ
D. WFQ

Answer: B

QUESTION 258
For scenario refer to iPAD document.
Which type of traffic receives the least amount of guaranteed bandwidth when exiting the S070 interface?

A. ftp
B. http
C. telnet
D. citrix

E. sqlnet

Answer: A

Mixed Questions (101 Questions)

QUESTION 259

```
!
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any VOICE-CONTROL
 match ip dscp cs3
 match ip dscp af31
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21
class-map match-all NETWORK-MANAGEMENT
 match ip dscp cs2
class-map match-all BULK-DATA
 match ip dscp af11
!
```

```
!
policy-map CE-EDGE
 class ROUTING
  bandwidth percent 3
 class VOICE
  priority percent 20
class MISSION-CRITICAL-DATA
  bandwidth percent 25
  random-detect dscp-based
  set ip dscp af31
class VOICE CONTROL
  priority percent 2
  set ip dscp cs5
class TRANSACTIONAL-DATA
  bandwidth percent 10
  random-detect dscp-based
  set ip dscp cs3
class NETWORK-MANAGEMENT
  bandwidth percent 2
  set ip dscp cs3
class BULK-DATA
  bandwidth percent 13
  random-detect dscp-based
  set ip dscp af21
class class-default
  fair-queue
!
```

Based on the configuration shown, which two of the following statements are correct? (Choose two)

A. All the different traffic classes are being re-marked into different DSCP values.
B. Both the VOICE and VOICE-CONTROL traffic classes will be serviced by the priority queue.
C. Both the TRANSACTION-DATA and NETWORK-MANAGEMENT traffic classes are being re-marked to CS3.
D. The ROUTING traffic class is policed by a congestion-aware policer.
E. Class-Based WRED is being implemented on all traffic classes.
F. Only 20% of the link bandwidth is guaranteed by the priority queue.

Answer: B, C

Explanation:
The MQC was originally introduced to support the configuration of Class-Based Weighted Fair Queuing (CBWFQ), but has now been expanded to include support for the configuration of nearly every QoS component. Although this list is not comprehensive, some of the QoS components that can be configured via the MQC include the following:
1. Traffic classification
2. Traffic marking
3. Congestion management
4. Congestion avoidance
5. Traffic conditioning
6. Header compression

End-to-end QoS deployment techniques for Cisco Catalyst series switches Examine various QoS components, including congestion management, congestion avoidance, shaping, policing/admission control, signaling, link efficiency mechanisms, and classification and marking Map specified class of service (CoS) values to various queues and maintain CoS values through the use of 802.1q tagging on the Cisco Catalyst 2900XL, 3500XL and Catalyst 4000 The fact that so many different components of QoS can be configured via the MQC, and the fact that each of the components previously listed has several possible mechanisms, makes the MQC one of the most versatile parts of Cisco IOS. When discussing technology, versatility usually means complexity, which is one of the amazing things about the MQC. The MQC was specifically designed to reduce configuration complexity and provide versatility.
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:
1. Class map configuration
2. Policy map configuration
3. Service policy application
The function of the class map is only to identify traffic, based on the characteristics given within the class map; the actual treatment of that traffic is specified in a policy map. As discussed earlier in the chapter, many different QoS mechanisms can be configured via the MQC, so the policy map has quite a few options. Note that, on switching platforms, not all of these options are supported in hardware. Switching platforms, such as the Catalyst 6500, may support some options in software. For performance reasons, you should not configure policies that are not supported in hardware unless absolutely necessary, because there could be a severe performance penalty for doing so. Cisco constantly adds new hardware support for features and the hardware support is different for different hardware (such as, PFC1 versus PFC2). As such, you should always check the hardware support for these actions before configuring them. NBAR was discussed earlier in this chapter and is a good example of something that was not supported in hardware on the 6500 at the time of this writing.
VOICE and VOICE-CONTROL configured with priority policy map option.
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.
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.
set- Allows for the marking of packets. Several fields can be marked through the use of the set command, including IP precedence, IP DSCP, MPLS experimental bits, Layer 2 CoS, the ATM cell loss priority (CLP) bit, and the QoS group.

QUESTION 260
The qos pre-classify command can be configured under which two configuration modes? (Choose two)

A. router(config)#
B. router(config-if)#
C. router(config-pmap-c)#
D. router(config-crypto-map)#
E. router(config-cmap)#
F. router(config-router)#

Answer: B, D

Explanation:
The QoS for VPNs feature, which is enabled by the qos pre-classify command, is restricted to tunnel and virtual template interfaces, and crypto map configuration submodes.
For generic routing encapsulation(GRE) and IP in IP(IPIP) tunnel protocols, the qos pre-classify command is applied on the tunnel interface, making QoS for VPNs a configuration option on a per-tunnel basis.
For Layer 2 Forwarding(L2F) and Layer 2 Tunneling Protocol(L2TP) protocols, the qos pre-classify command is applied on the virtual template interface. L2TP clients belonging to identical virtual private dial-up network (VPDN) groups inherit the preclassification setting. The qos pre-classify command can be configured on a per-VPDN tunnel basis.
For IPSec tunnels, the qos pre-classify command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption.
To configure the QoS for VPNs feature on a tunnel or virtual interface basis, use the following commands beginning in global interface mode:

	Command	Purpose
Step 1	Router(config)# **interface** [*tunnel-name* | *virtual-template-name*]	Enters interface configuration mode and specifies the tunnel or virtual interface to configure.
Step 2	Router(config-if)# **qos pre-classify**	Enables the QoS for VPNs feature.

To configure the QoS for VPNs feature on the crypto map configuration basis, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **crypto map** [*map-name*]	Enters crypto map configuration mode and specifies the previously defined crypto map to configure.
Step 2	Router(config-if)# **qos pre-classify**	Enables the QoS for VPNs feature.

QUESTION 261
Which element is mandatory for QoS policy propagation through BGP operations?

A. MPLS
B. NBAR
C. CEF

D. QoS pre-classify
E. Policy-based routing
F. MQC

Answer: C

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:
* Accurate accounting and the avoidance of double-accounting problems that were seen before "common classification".
* Reduces the impact of access control lists (ACLs) on the CPU since the ACL is checked once per class, rather than once per feature.
* Faster lookup of packet headers because of caching.
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:
1. Input rate-limiting, or CAR, applies to packets following the process switching path

and destined to the router. Previously, only packets switched through the router using CEF could be rate-limited.
2. New IP precedence values set by input CAR or QPPB can be used for selecting a Virtual Circuit (VC) in an ATM VC bundle.
3. IP precedence, Differentiated Services Code Points (DSCP), and QoS group values set by input CAR or QPPB can be used for MQC output packet classification.

QUESTION 262
What does the service-policy statement do?

A. Maps a type of traffic and QoS feature to an interface.
B. Maps a QoS feature to a type of traffic.
C. Differentiates types of traffic.
D. Differentiates QoS features.

Answer: A

Explanation:
For the service policy, only two options affect functionality: input and output. There is also a history option, not covered here in detail because it is for information only and does enable you to configure any functionality.
Example
R1(config-if)# service-policy ?
history Keep history of QoS metrics
input Assign policy-map to the input of an interface
output Assign policy-map to the output of an interface
The input option means that the policy map is applied to traffic that enters the router through this interface, and the output option means that the policy map is applied to traffic that leaves the router through this interface. The ability to apply a policy map input or output on a specific interface depends on which QoS mechanisms are used in the policy map. Some actions are only allowed in output policies.

QUESTION 263
Which configuration provides the mission-critical traffic class with a minimum bandwidth guarantee of 84 kbps and a maximum upper bandwidth limit of 96 kbps?

A. policy-map shape
class mission-critical
bandwidth 84
shape average 96000
B. policy-map shape
class mission-critical
bandwidth 96
shape average 64000
C. policy-map shape

class mission-critical
shape average 64000
shape peak 96000
D. policy-map shape
class mission-critical
priority 64
bandwidth 96

Answer: A

Explanation:
The function of the class map is only to identify traffic, based on the characteristics given within the class map; the actual treatment of that traffic is specified in a policy map. As discussed earlier in the chapter, many different QoS mechanisms can be configured via the MQC, so the policy map has quite a few options. Note that, on switching platforms, not all of these options are supported in hardware. Switching platforms, such as the Catalyst 6500, may support some options in software. For performance reasons, you should not configure policies that are not supported in hardware unless absolutely necessary, because there could be a severe performance penalty for doing so. Cisco constantly adds new hardware support for features and the hardware support is different for different hardware (such as, PFC1 versus PFC2). As such, you should always check the hardware support for these actions before configuring them.
Policy Map Options Available Under class
R1config-pmap-c)# ?
QoS policy-map class configuration commands:
exit Exit from QoS class action configuration mode
fair-queue Enable Flow-based Fair Queuing in this Class no Negate or set default values of a command
police Police
priority Strict Scheduling Priority for this Class
queue-limit Queue Max Threshold for Tail Drop
random-detect Enable Random Early Detection as drop policy
service-policy Configure QoS Service Policy
set Set QoS values
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.
shape- Allows for the configuration of class-based shaping, which is generic traffic shaping performed on a per-class basis. In this case, only the traffic in this class would be shaped. This is in contract to interface-based shaping, in which all traffic on the entire interface is shaped.

QUESTION 264
What is a PDLM (packet description language module) file?

A. It is used to enhance the list of protocols recognized by NBAR.

B. It is required file stored in the flash memory if the router when implementing class-based marking using NBAR.
C. It is used to enable the NBAR MIB for sending SMNP traps when the traffic rate hits a threshold.
D. It is used to store the application traffic statistics gathered by NBAR.
E. It is used to allow NBAR to search for a protocol using a port number other than the well-known port.
F. It is a file stored in the flash memory of the router and is used to integrate NBAR operations with auto-qos.

Answer: A

Explanation:
PDLMs provide the necessary information to the NBAR inspection process, allowing NBAR to recognize the various applications. PDLMs can be loaded into Flash, and do not require downtime for the system. As new PDLMs become available, they can be loaded on the Catalyst 6500 for additional protocol support. PDLMs are only available through Cisco.

QUESTION 265

```
Class-map well-known-services
   Match access-group 100
Class-map Unknown-services
   Match not class-map well-known-services
Policy-map set-DSCP
   Class well-known-services
      Set DSCP af21
   Class Unknown-services
      Set DSCP 1
!
Access-list 100 permit tcp any lt 1024
Access-list 100 permit tcp any lt 1024 any
!
Interface Ethernet 0/0
   Service-policy input set-DSCP
```

Given the above configuration, which two statements are correct? (Choose two)

A. All traffic not matching the well-known services class will be marked by the default-class to DSCP 0.
B. All traffic not matching either the well-known or unknown-services class will be marked by the default-class as DSCP 0.
C. All incoming DNS (port 53) traffic on Ethernet 0/0 will be marked af21.
D. All RTP applications (default ports 5004 and 5005) will be marked DSCP 1.
E. All Telnet (port 23) traffic exiting Ethernet 0/0 will be marked as af21.

Answer: C, D

Explanation:
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.
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
The match-any option is a logical OR operation, in which only one of the match conditions must be met for a packet to belong to a specific class. The
match-all option is a logical OR operation, in which all match criteria must be met for a packet to belong to a specific class. You must choose one of these options before you configure the remaining class map parameters.
This section discusses the various configuration parameters for the class map, followed by a configuration example. The distinction between match-any and match-all is discussed as part

---

QUESTION 266
What is the default trust mode on a Catalyst 2950 switch port?

A. trust cos
B. trust dscp
C. trust ip precedence
D. trust device cisco-phone
E. trust device cisco-router
F. untrusted

Answer: F

Explanation:
Auto-QoS
Auto-QoS eases the deployment of QoS on Catalyst switches by applying recommended QoS configuration for typical networks, especially those deploying VoIP. For the Catalyst 2950 Family and Catalyst 3550 Family of switches, the Auto-QoS feature, as

supported in 12.1.12c(EA1), aids in configuration of QoS for classification, egress scheduling, and congestion management of VoIP traffic for Cisco IP telephony. Upcoming software versions will offer additional Auto-QoS features.
Auto-QoS Classification
The Catalyst 2950 Family and 3550 Family of switches support two methods of classification when Auto-QoS is enabled. The first method classifies traffic strictly based on ingress CoS. Moreover, this configuration option just adds the trust CoS command to the interface for classification purposes. This method is useful for classifying traffic for interfaces connecting other switches.
The second method uses the trust Cisco IP Phone classification method as discussed in the "Trust Cisco IP Phone Device" section of this chapter. In brief, this method trusts ingress CoS only when a Cisco IP Phone is connected to an interface. This configuration option just adds the mls qos trust device cisco-phone and mls qos trust cos commands to the interface for classification.
To configure an interface for Auto-QoS of classification based on trust, use the following interface command:
auto qos voip trust
To configure an interface for Auto-QoS of classification based on trust and whether a Cisco IP phone is discovered on the interface, use the following interface command:
auto qos voip cisco-phone

QUESTION 267
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. priority
B. bandwidth
C. queue-limit
D. police
E. hold-queue

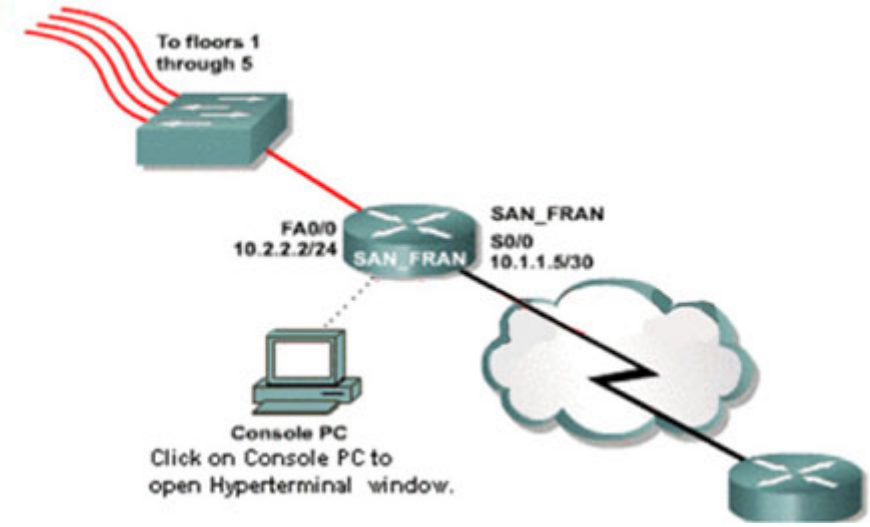
Answer: D

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 268
Exhibit:



What will happen if the incoming bulk class traffic rate arriving at the fa0/0 interface is higher than the normal burst rate (CIR)?

A. Dropped
B. Marked as AF11 then transmitted
C. Marked as DSCP 0 then transmitted.
D. Queued in the excess token buckert.
E. Queued in the CBWFQ.

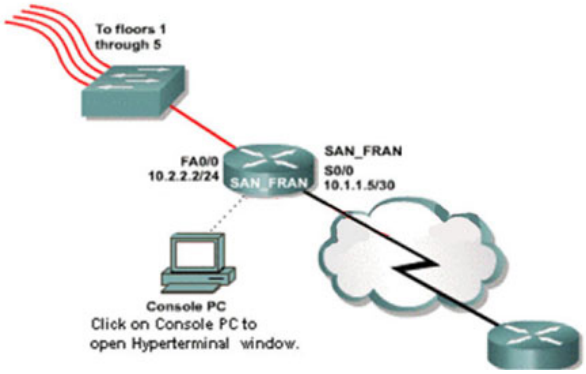
Answer: A

Explanation:
If the actual ingress traffic rate exceeds the configured rate, and there are insufficient tokens in the token bucket to accommodate the arriving traffic, the excess data is considered out-of-profile and can be dealt with in one of two ways:
1. Re-assign QoS values to appropriate header
2. Drop packet
If the decision is to mark down the nonconforming traffic, the DSCP value is derived from the mapping tables.
The token bucket mechanism has three components: a burst size, a mean rate, and a time interval (Tc). Although the mean rate is generally represented as bits per second, any two values may be derived from the

third by the relation shown as follows:
Mean rate = burst size / time interval
Here are some definitions of these terms:
Mean rate- Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.
Burst size- Also called the committed burst (Bc) size, it specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns. (For a shaper, such as generic traffic shaping (GTS), it specifies bits per burst; for a policer, such as committed access rate (CAR), it specifies bytes per burst.)
Time interval- Also called the measurement interval, it specifies the time quantum in seconds per burst. By definition, over any integral multiple of the interval, the bit rate of the interface will not exceed the mean rate. The bit rate, however, may be arbitrarily fast within the interval.
A token bucket is used to manage a device that regulates the data in a flow. For example, the regulator might be a traffic policer, such as CAR, or a traffic shaper, such as Frame Relay traffic shaping (FRTS) or GTS. A token bucket itself has no discard or priority policy. Rather, a token bucket discards tokens and leaves to the flow the problem of managing its transmission queue if the flow overdrives the regulator. (Neither CAR nor FRTS and GTS implement either a true token bucket or true leaky

---

QUESTION 269
Exhibit:



All traffic belonging to the class-default traffic class on the s0/0 interface will be queued by a class queue that uses which type of queuing?

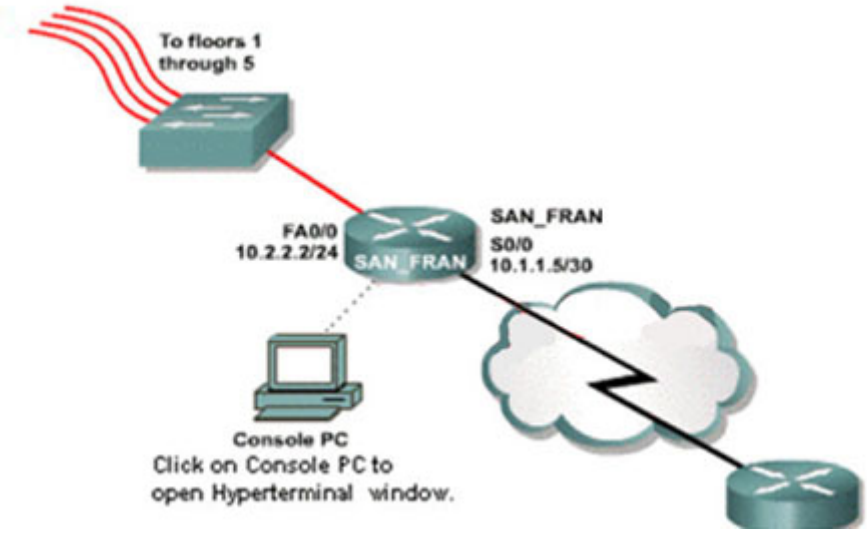
A. FIFO
B. LLQ
C. WFQ
D. Round Robin
E. PQ

Answer: A

Explanation:
Originally, the queuing mechanism on all interfaces was first-in, first-out (FIFO), meaning that the first packet to arrive for transmission would be the first packet transmitted, the fifth packet arriving would be the fifth packets transmitted, and so on. This queuing mechanism works just fine if all of your traffic has no delay concerns

(perhaps FTP or other batch transfer traffic). If you've ever worked with data-link switching (DLSw), however, you know how sensitive that traffic is to delay in the network.
For many networks, the first real need for QoS was to allow for priority treatment of DLSw traffic over low-speed WAN links. The need to provide basic prioritization of different types of data traffic was first seen in the WAN, because that is where bandwidth is most limited. In the case of Priority Queuing, the need was to prioritize a single traffic type (or a select few types of traffic) over all others. Custom Queuing addressed the need to provide basic bandwidth sharing, and Weighted Fair Queuing provided the ability to dynamically allocate more or less bandwidth to a given flow based on the IP precedence of the packets in that flow. Class-Based Weighted Fair Queuing (CBWFQ) and Low Latency Queuing (LLQ) are hybrid QoS mechanisms-that is, they provide a combination of the other functions to allow for greater flexibility.

QUESTION 270
Exhibit:



What will happen if the incoming mission-critical class traffic rate arriving at the fa0/0 interface is higher than the normal burst rate (CIR) but not exceeding the excess burst rate?

A. Dropped
B. Marked as AF31 then transmitted.
C. Marked as AF32 then transmitted.
D. Marked as AF33 then transmitted.
E. Queued in the CBWFQ.

Answer: D

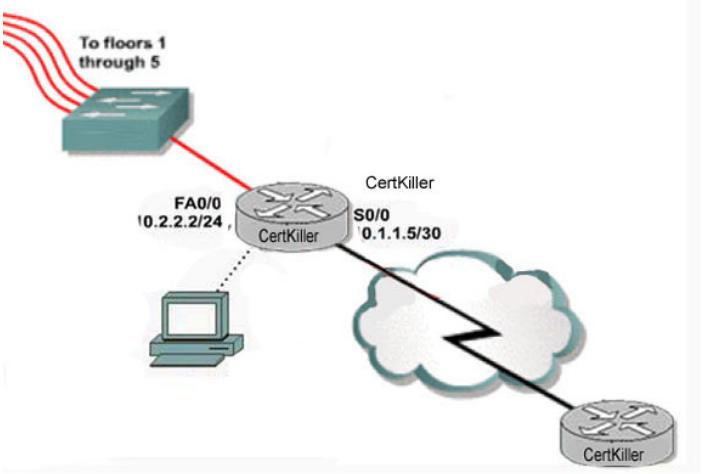
Explanation:
Other than those defined in RFC 2474, there are two main PHBs, RFC 2597 defines the first of these. It is called the assured forwarding (AF) PHB, and the concept behind the

PHB is to provide a level of assurance as to a given packet's probability of being forwarded during congestion. RFC 2597 defines four classes, and each class is completely independent of the other classes. In addition, each class has three level of "drop precedence" to which packets of that class can be assigned.
From a high level, the concept is that you can have four different classes of traffic and, within those classes, you can have three different levels of probability that a packet will be dropped if that class becomes congested.

Table 2-7. Codepoint Markings for the AF PHB

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	AF11 (001010) 10	AF21 (010010) 18	AF31 (011010) 26	AF41 (100010) 34
Medium	AF12 (001100) 12	AF22 (010100) 20	AF32 (011100) 28	AF42 (100100) 36
High	AF13 (001110) 14	AF23 (010110) 22	AF33 (011110) 30	AF43 (100110) 38

QUESTION 271
Exhibit:



Which type of traffic receives the least amount of guaranteed bandwidth when exiting the S0/0 interface?

A. ftp
B. http
C. telnet
D. citrix
E. sqlnet

Answer: A

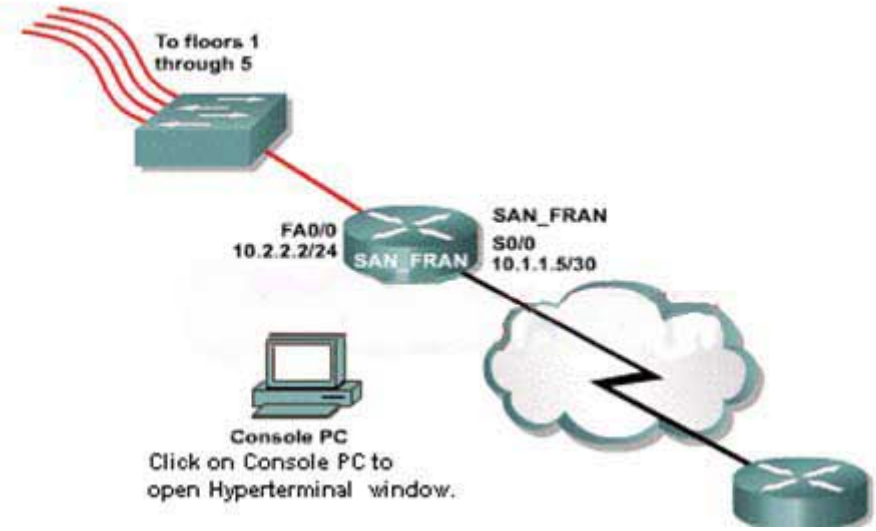
Explanation:

Table 2-7. Codepoint Markings for the AF PHB

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	AF11 (001010) 10	AF21 (010010) 18	AF31 (011010) 26	AF41 (100010) 34
Medium	AF12 (001100) 12	AF22 (010100) 20	AF32 (011100) 28	AF42 (100100) 36
High	AF13 (001110) 14	AF23 (010110) 22	AF33 (011110) 30	AF43 (100110) 38

To understand a possible use for the AF PHB, assume that you have four branch offices aggregating into a single router. Each branch has been told that they should not send more than 256 kbps of FTP traffic, but sometimes they do anyway. In fact, sometimes they send more than 1 Mbps of FTP traffic. The problem is that when one branch sends a lot of FTP traffic, it sometimes interferes with another branch's FTP traffic, even if they are sending at or below the 256-kbps limit.

QUESTION 272
Exhibit:



Which type of software queue is used on the s0/0 interface?

A. LLQ
B. CBWFQ
C. FIFO
D. WFQ

Answer: B

Explanation:
Weighted Fair Queuing

Weighted Fair Queuing (WFQ) is a dynamic process that divides bandwidth among queues based on weights. The process is designed to be fair, such that WFQ ensures that all traffic is treated fairly, with regard to its weight.
There are several forms of WFQ, including Class-based Weighted Fair Queuing (CBWFQ) and Low Latency Queuing (LLQ).
CBWFQ is probably the form of WFQ that is most commonly being deployed these days. CBWFQ works quite a bit like CQ, but the algorithm is more efficient and the configuration is quite a bit easier to understand. With CBWFQ, classes are created and traffic is assigned to those classes, as explained earlier in this chapter. Bandwidth is then assigned to those classes, and the amount of bandwidth assigned to a given class determines the amount of scheduling that class receives.
In other words, the bandwidth statement on a given class determines the minimum amount of bandwidth that packets belonging to that class receive in the event of congestion. In the recent past, a PQ was added to the CBWFQ mechanism, specifically to handle VoIP traffic. This addition was necessary because, although CBWFQ did an excellent job of dividing up the available bandwidth, CBWFQ did not give any specific regard to the delay or jitter being introduced by queuing packets.
The LLQ mechanism is CBWFQ with a single PQ, which receives strict scheduling priority. To go back to airline analogies, this is the equivalent of preboarding courtesies that are often offered to persons with special needs or those traveling with small children. In spite of the fact that these people may not be in first class, or elite frequent fliers, they are moved directly to the front of the line and put on the plane first because they have special needs. In the case of VoIP traffic, it may not be the most important traffic on your network, but it has very specific requirements for delay and jitter and, therefore, must be moved to the front of the line for transmission.
Catalyst switches use classification to appropriate queuing frames for transmission. Although Catalyst switches only support the Cisco IOS features WFQ, CBWFQ, and LLQ on WAN interfaces, Ethernet interfaces use similar forms of queuing but vary in configuration and behavior.

QUESTION 273
DRAG DROP
Drag each traffic type to its QoS markings on the right based on Cisco's recommendation for traffic classifications and markings.

routing	EF	Place here
voice	CS1	Place here
mission-critical data	CS2	Place here
call signaling	CS3	Place here
bulk	CS6	Place here
scavanger	AF31	Place here
best effort	AF11	Place here
network management	0	Place here

Answer:

QUESTION 274
With a queue depth at maximum threshold, its is desired that one out of every 512 packets be dropped. In this case, what is the number 512 known as?

A. Mark probability denominator
B. Congestive discard threshold
C. Minimum-drop threshold
D. Maximum-drop threshold

Answer: A

QUESTION 275
AutoQos is which type of Cisco IOS command?

A. interface
B. global
C. policy-map
D. service-map
E. serial interface only

Answer: A

Explanation:
Cisco AutoQos represents innovative technology that simplifies the challenges of network administration by reducing QoS complexity, deployment time and cost in 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 deployements.
Then First phase of Cisco AutoQoS offers straight forward capabilities to automate VoIP deployments for customers who want to deploy IP telephony but lack the expertise and staffing to plan and deploy IP QoS and IP Services.

The AutoQoS VoIP feature simplifies QoS implementation and speeds up the provisioning of QoS technology over a Cisco network. It also reduces human error and lowers training costs. With the AutoQoS VOIP feature, one command (auto qos) enables QoS for VoIP traffic across every Cisco Router and Switch.

QUESTION 276
Which two of the following statements about CBWFQ are correct? (Choose two)

A. The CBWFQ scheduler provides a guaranteed amount of minimum bandwidth to each class.
B. CBWFQ services each class queue using a strict priority scheduler.
C. The class-default queue only supports WFQ.
D. Each CBWFQ traffic class is policed using a congestion aware policer.
E. Inside a class queue, processing is always FIFO, except for the class-default queue.

Answer: A, E

Explanation:
A protocol-dependent switching process handles traffic arriving at a router interface. The switching process includes delivery of traffic to an outgoing interface buffer. First-in, first-out (FIFO) queuing is the classic algorithm for packet transmission. With FIFO, transmission occurs in the same order as messages are received. Until recently, FIFO queuing was the default for all router interfaces. If users require traffic to be reordered, the department or company must establish a queuing policy other than FIFO queuing.
Cisco IOS software offers three alternative queuing options:
1. Weighted fair queuing (WFQ) prioritizes interactive traffic over file transfers in order to ensure satisfactory response time for common user applications.
2. Class-based weighted fair queuing (CBWFQ) in IOS 12.2 prioritizes traffic based on user-defined classes.
3. Low latency queuing (LLQ) (IOS 12.2) brings strict priority queueing to Class-Based Weighted Fair Queuing (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.

QUESTION 277
Which of the following configurations requires the use of hierarchical policy maps?

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

Answer: C

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 278
An ECN-enabled packet arrives at a router with ECN WRED turned on. WRED determines the packet should be dropped. What happens when the average queue length is between the minimum and maximum thresholds?

A. The packet is tail dropped.
B. The packet is forwarded without change in all cases.

C. The ECT and CE bits are set to 1 if not already set.
D. The ECT bit is set to 0 and the CE bit is set to 1 of not already set.

Answer: C

Explanation:
The figure shows how weighted random early detect (WRED) is implemented, and what parameters influence WRED dropping decisions. The WRED algorithm is constantly updated with the calculated average queue size, which is based on the recent history of queue sizes.
The configured WRED profiles define the dropping thresholds. When a packet arrives at the output queue, the IP Precedence of the Differentiated Services Code Point (DSCP) value is used to select the correct WRED profile for the packet. The packet is then passed to WRED to perform a drop/enqueue decision.
Based on the profile and the average queue size, WRED calculates the probability for dropping the current packet and either drops it or passes it to the output queue. If the queue is already full, the packet is tail-dropped. Otherwise, it is eventually sent out on the interface.
WRED monitors the average queue depth in the router and determines when to begin packet drops based on the queue depth. When the average queue depth crosses the user-specified minimum threshold, WRED begins to drop both TCP and UDP packets with a certain probability.
If the average queue depth ever crosses the user-specified maximum threshold, then WRED reverts to tail drop, and all incoming packets might be dropped. The idea behind using WRED is to maintain the queue depth at a level somewhere between the minimum and maximum thresholds, and to implement different drop policies for different classes of traffic.
WRED is only useful 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. Dropping packets may not decrease congestion.
WRED can be used wherever there is a potential bottleneck or congested link at the access/edge link of the network. However, WRED is normally used in the core routers of a network rather than at the network edge. Edge routers assign IP Precedences to packets as they enter the network. WRED uses these IP Precedences to determine how to treat different types of traffic.

QUESTION 279
With the use of class maps to classify traffic, into which traffic class will the majority of the enterprise traffic typically be classified?

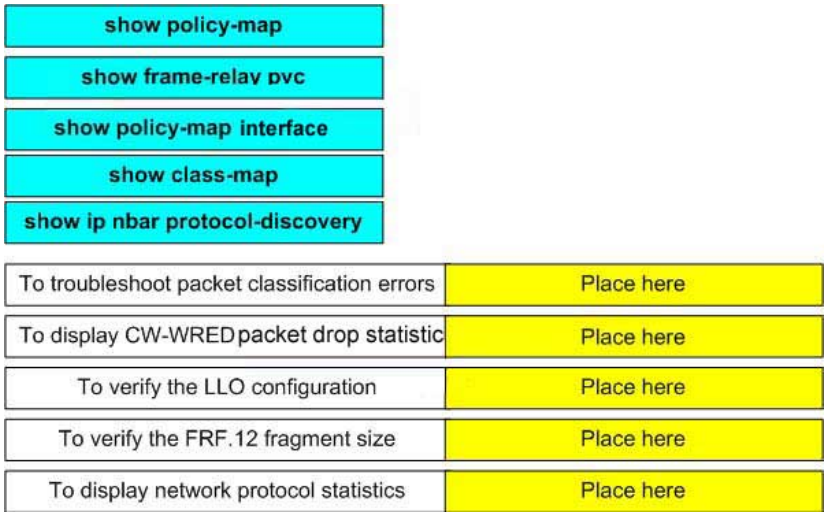
A. priority
B. bulk
C. mission-critical
D. transactional
E. class-default

F. scavenger

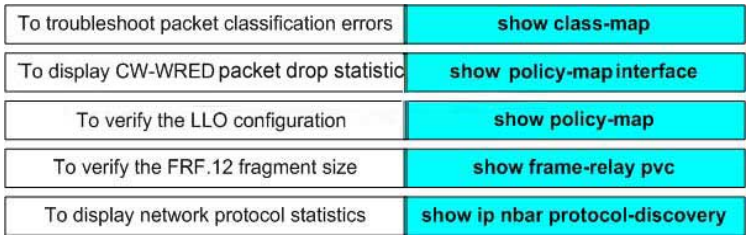
Answer: E

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.
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:
1. Policy Name
2. Traffic class specified with the class command
3. QoS policies to be applied to each class
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 policy1
Switch(config-pmap)#class cisco
Switch(config-pmap-c)#bandwidth 3000
Switch(config-pmap-c)#exit
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#bandwidth 2000
Switch(config-pmap)#exit

QUESTION 280
DRAG DROP
Match the correct show command to the given scenario.



Answer:



Explanation:

1. The output from show class-map displays all the configured classes, whether classes are a match-any or a match-all class, what the name of each class is, and which traffic belongs in those classes. Overall, this is a very useful command.

Also notice the class-default, which is automatically created whenever any other class is created. The purpose of class-default is to give all traffic that does not belong to any other class a place to go.

2. There is a command to show the interface specific policy map information, and you should use that command to view the details of the policy map after it has been applied to an interface.

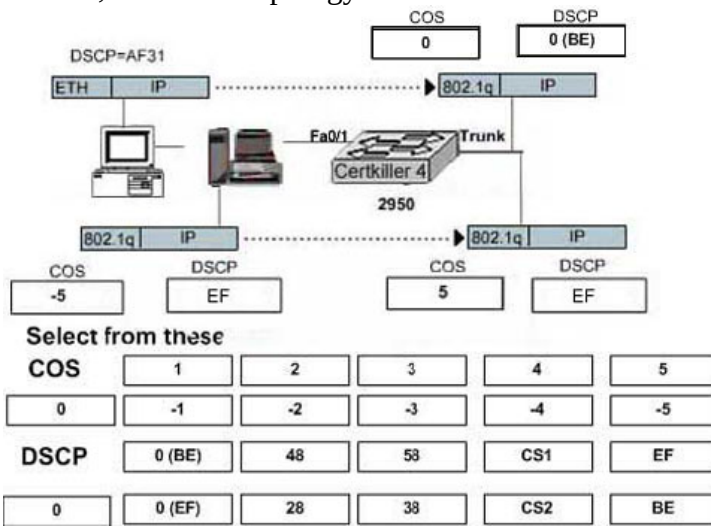
R1# show policy-map interface serial 1/0
Serial1/0
Service-policy output: ACCOUNTING-POLICY
Class-map: ACCOUNTING-HTTP (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 101
Match: access-group 103
Queueing
Output Queue: Conversation 265
Bandwidth 128 (kbps) Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0
Class-map: ACCOUNTING-FTP (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 102

Match: access-group 103
Queueing
Output Queue: Conversation 266
Bandwidth 128 (kbps) Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0
Traffic Shaping
Target/Average Byte Sustain Excess Interval Increment
Rate Limit bits/int bits/int (ms) (bytes)
256000/256000 1984 7936 7936 31 992
Adapt Queue Packets Bytes Packets Bytes Shaping
3. You can confirm the configuration that has been entered through the use of the show policymap command, Example:
R1# show policy-map
Policy Map ACCOUNTING-POLICY
Class ACCOUNTING-HTTP
Bandwidth 128 (kbps) Max Threshold 64 (packets)
Class ACCOUNTING-FTP
Bandwidth 128 (kbps) Max Threshold 64 (packets)
Class DEVELOPMENT-HTTP
Bandwidth 64 (kbps) Max Threshold 64 (packets)
Class DEVELOPMENT-FTP
Bandwidth 32 (kbps) Max Threshold 64 (packets)
Class class-default
As indicated by the output, the queue limit for each of these classes is set to 64 packets (the default). This output also shows the policy map's name, the names of all the class maps within the policy, and the policy that has actually been configured for each class. Notice that this command does not show any information about the traffic that will belong to each class or whether each class is a match-any or a match-all.
4. The show frame-relay pvc command displays the status of each configured connection, as well as traffic statistics. This command is also useful for viewing the number of Backward Explicit Congestion Notification (BECN) and Forward Explicit Congestion Notification (FECN) packets received by the router.
5. The first step in being able to classify network traffic is to actually know what protocols and applications are running on the network. This knowledge enables administrators to prioritize business-critical information and applications over less-important applications. Unfortunately, to configure ACLs to classify network traffic you must have prior knowledge of the network applications, as well as their associated protocol or port numbers. One option for discovering the protocols currently traversing an interface within the network is using NBAR protocol discovery. NBAR is capable of recognizing any protocol included within the PDLM file. Protocol discovery is applied to the desired interface or group of interfaces using the following command at each intended interface:
ip nbar protocol-discovery
When protocol discovery is applied to the interface, statistics are gathered depicting the active protocols traversing the interface. To view the results of the protocol discovery process, use the following command:
show ip nbar protocol-discovery [interface type num]

QUESTION 281
DRAG DROP
Exhibit, 2950 configuration

```
! 2950 config
mls qos map cos-dscp 0 10 18 26 34 40 48 56
Interface fa0/1
  mls qos trust  cos
  mls qos trust device cisco-phone
  switchport priority extend cos 0
  wrr-queue cos-map 4 5
  wrr-queue bandwidth 20 1 80 0
```

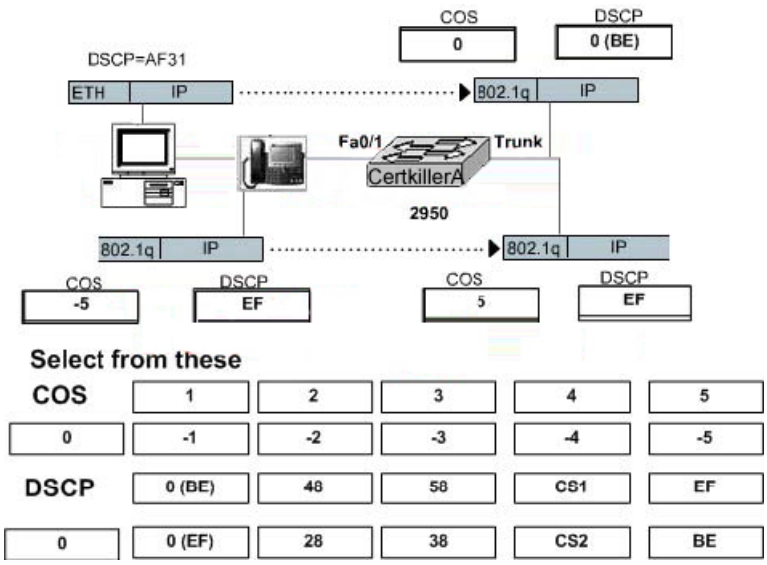
Exhibit, Network Topology



You work as a technician at Certkiller .com. Based on the topology in the exhibit and the 2950 configuration shown, select the appropriate COS and DSCP values from down boxes for the packets below. The top set of packets are the PC generated packet. The bottom of packets are the Cisco's IP Phone generated packet.

Answer:

Explanation:



The router config contains the line:
Switchport priority extend cos 0
Which tells the phone to override the cos values on any packets received from the workstation before sending it on to the switch.
The router config contains the line:
Mls qos trust device cisco-phone
Which tells the switch to trust any cos/dscp values received from an attached cisco phone.
You see that the workstation is generating packets with a dscp value of af31, when it hits the phone the phone will rewrite the cos value to 0, which is the same as dscp value of 0(BE).

QUESTION 282
What are the three steps involved in implementing a QoS policy using MQC?
(Choose three)

A. Define a policy map.
B. Define a traffic class.
C. Set the match parameters for a policy map.
D. Define a route map to set the QoS markings.
E. Assign a service policy to an interface.

Answer: A, B, E

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

QUESTION 283
The show policy-map interface command output is showing too many random drops for the mission-critical traffic class. What can be changed to reduce the random drops?

A. Increase the WRED max-threshold value for the mission-critical traffic class.
B. Increase the WRED min-threshold value for the mission-critical traffic class.
C. Decrease the WRED drop probability denominator for the mission-critical traffic class.
D. Decrease the queue-limit for the mission-critical traffic class.
E. Enable fair-queue within the mission-critical traffic class.

Answer: B

Explanation:
Weighted Fair Queuing (WFQ) is a dynamic process that divides bandwidth among queues based on weights. The process is designed to be fair, such that WFQ ensures that all traffic is treated fairly, with regard to its weight.
There are several forms of WFQ, including Class-based Weighted Fair Queuing (CBWFQ) and Low Latency Queuing (LLQ).
CBWFQ is probably the form of WFQ that is most commonly being deployed these days. CBWFQ works quite a bit like CQ, but the algorithm is more efficient and the configuration is quite a bit easier to understand. With CBWFQ, classes are created and traffic is assigned to those classes, as explained earlier in this chapter. Bandwidth is then assigned to those classes, and the amount of bandwidth assigned to a given class determines the amount of scheduling that class receives.
In other words, the bandwidth statement on a given class determines the minimum amount of bandwidth that packets belonging to that class receive in the event of congestion.
In the recent past, a PQ was added to the CBWFQ mechanism, specifically to handle VoIP traffic. This addition was necessary because, although CBWFQ did an excellent job of dividing up the available bandwidth, CBWFQ did not give any specific regard to the delay or jitter being introduced by queuing packets.
The LLQ mechanism is CBWFQ with a single PQ, which receives strict scheduling priority. To go back to airline analogies, this is the equivalent of preboarding courtesies that are often offered to persons with special needs or those traveling with small children. In spite of the fact that these people may not be in first class, or elite frequent fliers, they are moved directly to the front of the line and put on the plane first because they have special needs. In the case of VoIP traffic, it may not be the most important traffic on your network, but it has very specific requirements for delay and jitter and, therefore, must be moved to the front of the line for transmission.
Catalyst switches use classification to appropriate queuing frames for transmission. Although Catalyst switches only support the Cisco IOS features WFQ, CBWFQ, and

LLQ on WAN interfaces, Ethernet interfaces use similar forms of queuing but vary in configuration and behavior.

QUESTION 284
For which service is assured forwarding PHB used?

A. Best effort
B. Expedited forwarding
C. Guaranteed bandwidth
D. Class selector

Answer: C

Explanation:
With the introduction of the DSCP markings, there were significantly more possible markings for packets (0-63 are the possible markings for packets). Because there were so many more possible markings, the IETF decided to standardize what some of the codepoints meant. In part, this is to provide backward compatibility to IP precedence and, in part, this is to facilitate certain types of behaviors that were seen as fundamental to the DiffServ architecture.
The following definition of a per-hop behavior is taken from Section 2.4 of RFC 2475:
A per-hop behavior (PHB) is a description of the externally observable forwarding behavior of a DS node applied to a particular DS behavior aggregate ... In general, the observable behavior of a PHB may depend on certain constraints on the traffic characteristics of the associated behavior aggregate, or the characteristics of other behavior aggregates.
RFC 2597: The Assured Forwarding PHB
Other than those defined in RFC 2474, there are two main PHBs, RFC 2597 defines the first of these. It is called the assured forwarding (AF) PHB, and the concept behind the PHB is to provide a level of assurance as to a given packet's probability of being forwarded during congestion.
RFC 2597 defines four classes, and each class is completely independent of the other classes. In addition, each class has three level of "drop precedence" to which packets of that class can be assigned.

QUESTION 285
What are the two queuing options to the Catalyst 2950? (Choose two)

A. IP3Q
B. 2P2Q
C. 4Q
D. 1P2QIT

Answer: A, C

QUESTION 286
What is the class selector PHB used for in the differentiated services model?

A. Best-effort service
B. Low-delay service
C. Bandwidth guarantee
D. Backward compatibility

Answer: D

Explanation:
With the introduction of the DSCP markings, there were significantly more possible markings for packets (0-63 are the possible markings for packets). Because there were so many more possible markings, the IETF decided to standardize what some of the codepoints meant. In part, this is to provide backward compatibility to IP precedence and, in part, this is to facilitate certain types of behaviors that were seen as fundamental to the DiffServ architecture.
The following definition of a per-hop behavior is taken from Section 2.4 of RFC 2475:
A per-hop behavior (PHB) is a description of the externally observable forwarding behavior of a DS node applied to a particular DS behavior aggregate ... In general, the observable behavior of a PHB may depend on certain constraints on the traffic characteristics of the associated behavior aggregate, or the characteristics of other behavior aggregates.
RFC 2597: The Assured Forwarding PHB
Other than those defined in RFC 2474, there are two main PHBs, RFC 2597 defines the first of these. It is called the assured forwarding (AF) PHB, and the concept behind the PHB is to provide a level of assurance as to a given packet's probability of being forwarded during congestion.
RFC 2597 defines four classes, and each class is completely independent of the other classes. In addition, each class has three level of "drop precedence" to which packets of that class can be assigned.

QUESTION 287
DRAG DROP
Match the IOS QoS feature on the left to the appropriate QoS mechanism on the right.

FRF.12	Classification and marking	Place here
QPPB	Link fragmentation and interleaving	Place here
LLQ	Trafic conditioner	Place here
WRED	Congestion management	Place here
class-based policer	Congestion avoidance	Place here

Answer:

Classification and marking	QPPB
Link fragmentation and interleaving	FRF.12
Traffic conditioner	class-based policer
Congestion management	LLQ
Congestion avoidance	WRED

Explanation:
A protocol-dependent switching process handles traffic arriving at a router interface. The switching process includes delivery of traffic to an outgoing interface buffer. First-in, first-out (FIFO) queuing is the classic algorithm for packet transmission. With FIFO, transmission occurs in the same order as messages are received. Until recently, FIFO queuing was the default for all router interfaces. If users require traffic to be reordered, the department or company must establish a queuing policy other than FIFO queuing. Cisco IOS software offers three alternative queuing options:
1. Weighted fair queuing (WFQ) prioritizes interactive traffic over file transfers in order to ensure satisfactory response time for common user applications.
2. Class-based weighted fair queuing (CBWFQ) in IOS 12.2 prioritizes traffic based on user-defined classes.
3. Low latency queuing (LLQ) (IOS 12.2) brings strict priority queueing to Class-Based Weighted Fair Queuing (CBWFQ).

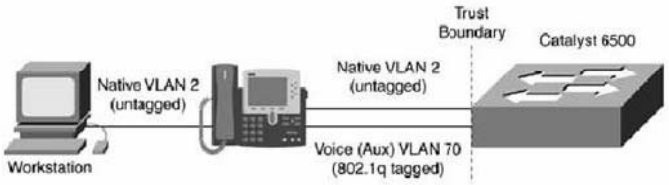
QUESTION 288
Which other protocol does the auto qos voip cisco-phone command require to operate between the switch port and the IP phone?

A. RTP
B. Skinny Protocol
C. CDP
D. RTCP
E. VTP
F. DTP

Answer: C

Explanation:
Through the use of dot1q trunks, voice traffic from an IP Phone connected to an access port can reside on a separate VLAN and subnet. The workstation attached to the IP Phone might still reside on the access, or native, VLAN. This additional VLAN on an access port for voice traffic is referred to as a voice VLAN in Cisco IOS Software and auxiliary VLAN in CatOS. Subsequently, with the use of voice VLANs, all voice traffic is tagged to and from the Cisco IP Phone and Catalyst switch. The Catalyst switches use Cisco

Discovery Protocol (CDP) to inform the IP Phone of the voice VLAN ID. By default, Cisco IP Phone voice traffic has a CoS value of 5. Here an example logical depiction of a voice VLAN. A common network design is to deploy both voice VLANs with trusting configurations for Cisco IP telephony applications (such as Cisco IP Phones).



Another QoS option for IP Phones is extended trust. The switch can inform the IP Phone via CDP whether to trust ingress frames on its P1 port. The IP Phone may also be informed to overwrite the CoS value of the ingress frames on the P1 port with a specific CoS value. By default, the IP Phone does not trust frames arriving on the P1 port and rewrites the CoS value to 0 of any tagged frames. Untagged frames do not have CoS value.
Extended trust is a feature available to any device that can interpret the CDP fields describing the voice VLAN information. At the time of publication, Cisco IP Phones and other Cisco appliances are the only devices to use this feature.

QUESTION 289
What are the four types of per-hop behavior used with DSCP? (Choose four)

A. Expedited forwarding
B. Default
C. Class-bit
D. Assured forwarding
E. Class-selector
F. Express forwarding

Answer: A, B, D, E

Explanation:
With the introduction of the DSCP markings, there were significantly more possible markings for packets (0-63 are the possible markings for packets). Because there were so many more possible markings, the IETF decided to standardize what some of the codepoints meant. In part, this is to provide backward compatibility to IP precedence and, in part, this is to facilitate certain types of behaviors that were seen as fundamental to the DiffServ architecture.
The following definition of a per-hop behavior is taken from Section 2.4 of RFC 2475:
A per-hop behavior (PHB) is a description of the externally observable forwarding behavior of a DS node applied to a particular DS behavior aggregate ... In general, the observable behavior of a PHB may depend on certain constraints on the traffic characteristics of the associated behavior aggregate, or the characteristics of other behavior aggregates.
RFC 2597: The Assured Forwarding PHB
Other than those defined in RFC 2474, there are two main PHBs, RFC 2597 defines the

first of these. It is called the assured forwarding (AF) PHB, and the concept behind the PHB is to provide a level of assurance as to a given packet's probability of being forwarded during congestion.
RFC 2597 defines four classes, and each class is completely independent of the other classes. In addition, each class has three level of "drop precedence" to which packets of that class can be assigned.
Expedited Forwarding (EF) PHB:
- Ensures minimum departure rate
- Guarantees bandwidth : The class is guaranteed an amount of bandwidth with prioritized forwarding
- Policies bandwidth : The class is not allowed to exceed the guaranteed amount
- Packets requiring Expedited Forwarding should be marked with DSCP binary Value.

Table 2-6. Backward Compatibility with IP Precedence Values

Bits	Precedence
001000	Class selector 1; read as 001 by a non-DiffServ node and treated like IP precedence 1.
010000	Class selector 2; read as 010 by a non-DiffServ node and treated like IP precedence 2.
011000	Class selector 3; read as 011 by a non-DiffServ node and treated like IP precedence 3.
100000	Class selector 4; read as 100 by a non-DiffServ node and treated like IP precedence 4.
101000	Class selector 5; read as 101 by a non-DiffServ node and treated like IP precedence 5.
110000	Class selector 6; read as 110 by a non-DiffServ node and treated like IP precedence 6.
111000	Class selector 1; read as 111 by a non-DiffServ node and treated like IP precedence 7.

QUESTION 290
Which four of the following are required to calculate the LLQ priority bandwidth requirement for the voice traffic class? (Choose three)

A. Codec type
B. IP/UDP/RTP header lengths and Layer 2 overhead.
C. IP Phone Skinny Protocol overhead.
D. Number of concurrent VoIP calls to support.
E. Voice digitalization overhead.

Answer: A, B, D, F

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.
Although it is possible to enqueue various types of real-time traffic to the strict priority queue, Cisco recommends that only voice traffic be directed to it. This recommendation is made because voice traffic is well-behaved, whereas other types of real-time traffic are not. Moreover, voice traffic requires that delay be nonvariable in order to avoid jitter. Real-time traffic such as video could introduce variation in delay, thereby disrupting the steadiness of delay required for successful voice traffic transmission.

QUESTION 291
Which binary pattern is a valid class selector PHB DSCP value?

A. 110001
B. 000010
C. 111000
D. 000001

Answer: C

Explanation:
With the introduction of the DSCP markings, there were significantly more possible markings for packets (0-63 are the possible markings for packets). Because there were so many more possible markings, the IETF decided to standardize what some of the codepoints meant. In part, this is to provide backward compatibility to IP precedence and, in part, this is to facilitate certain types of behaviors that were seen as fundamental to the DiffServ architecture.
The following definition of a per-hop behavior is taken from Section 2.4 of RFC 2475:
A per-hop behavior (PHB) is a description of the externally observable forwarding behavior of a DS node applied to a particular DS behavior aggregate ... In general, the observable behavior of a PHB may depend on certain constraints on the traffic characteristics of the associated behavior aggregate, or the characteristics of other behavior aggregates.
RFC 2597: The Assured Forwarding PHB
Other than those defined in RFC 2474, there are two main PHBs, RFC 2597 defines the first of these. It is called the assured forwarding (AF) PHB, and the concept behind the PHB is to provide a level of assurance as to a given packet's probability of being

forwarded during congestion.
RFC 2597 defines four classes, and each class is completely independent of the other classes. In addition, each class has three level of "drop precedence" to which packets of that class can be assigned.
Expedited Forwarding (EF) PHB:
- Ensures minimum departure rate
- Guarantees bandwidth : The class is guaranteed an amount of bandwidth with prioritized forwarding
- Policies bandwidth : The class is not allowed to exceed the guaranteed amount
- Packets requiring Expedited Forwarding should be marked with DSCP binary Value.

QUESTION 292
When configuring WFQ, what is the default number of dynamic queues based on?

A. hold-queue limit
B. congestive discard threshold (CDT)
C. interface bandwidth
D. hash of the packet headers
E. inter-packet arrival rate
F. drop probability denominator

Answer: C

Explanation:
Weighted Fair Queuing (WFQ) classifies traffic entering the queue based on traffic flows. The actual classification can be based on source and destination addresses, the protocol and TCP port numbers. Each flow is given its own queue. In its simplest form WFQ services each of these queues on a round robin basis. This means that every flow of traffic has an equal share of the available bandwidth, if it is required. Hence the term "fair" queue. The benefit for low volume traffic is reduced and predictable latency. For many applications this default behavior of WFQ is sufficient, however, some applications need specific QoS guarantees that require more than simply "fair" access to the bandwidth. In this case, the "weight" needs to be modified so that WFQ does not share bandwidth on a round-robin basis, but is influenced by the class or priority of the traffic in the flow.
Weighted fair queuing is activated on an interface using the fair-queue command:
Router(config)#interface serial 0/0
Router(config-if)#fair-queue
Note that the queuing strategies described here apply to packets at Layer 3. Consequently, these techniques can only be used on router interfaces. Physical interfaces on the Catalyst 3550 and Catalyst 6500 switches are used as router interfaces after applying the command:
switch(config-if)#no switchport
These features are not available on regular Layer 2 switch ports and none of these features are available on Layer 2 switches such as the Catalyst 2950.

QUESTION 293
Traffic classification using NBAR is configured using which IOS command?

A. router(config-cmap)# match protocol {protocol-name}
B. router(config-if)# ip nbar protocol-discovery
C. router(config)# ip nbar port-map {protocol} [tcp|udp] {port-number} {port-number}...
D. router(config)# ip nbar pdlm {pdlm-file}

Answer: A

Explanation:
protocol- Allows for the matching of certain predefined protocols. Network-based application recognition (NBAR) is a new classification engine that can recognize a large number of applications based on both static and dynamically assigned port numbers. On routers that support NBAR, the list of protocols is extensive,
R1(config-cmap)# match protocol ?
aarp AppleTalk ARP
apollo Apollo Domain
appletalk AppleTalk
arp IP ARP
bgp Border Gateway Protocol
bridge Bridging
bstun Block Serial Tunnel
cdp Cisco Discovery Protocol
citrix Citrix Traffic
clns ISO CLNS
clns_es ISO CLNS End System
clns_is ISO CLNS Intermediate System
cmns ISO CMNS
compressedtcp Compressed TCP
cuseeme CU-SeeMe desktop video conference
custom-01 Custom protocol custom-01
custom-02 Custom protocol custom-02
custom-03 Custom protocol custom-03
custom-04 Custom protocol custom-04
custom-05 Custom protocol custom-05
custom-06 Custom protocol custom-06
custom-07 Custom protocol custom-07
custom-08 Custom protocol custom-08
custom-09 Custom protocol custom-09
custom-10 Custom protocol custom-10
decnet DECnet
decnet_node DECnet Node
decnet_router-l1 DECnet Router L1
decnet_router-l2 DECnet Router L2

dhcp Dynamic Host Configuration
dlsw Data Link Switching
dns Domain Name Server lookup
egp Exterior Gateway Protocol
eigrp Enhanced Interior Gateway Routing Protocol
exchange MS-RPC for Exchange
fasttrack FastTrack Traffic - KaZaA, Morpheus, Grokster...
finger Finger
ftp File Transfer Protocol
gnutella Gnutella Traffic - BearShare,LimeWire, Gnutella...
gopher Gopher
gre Generic Routing Encapsulation
http World Wide Web traffic
icmp Internet Control Message
imap Internet Message Access Protocol
ip IP

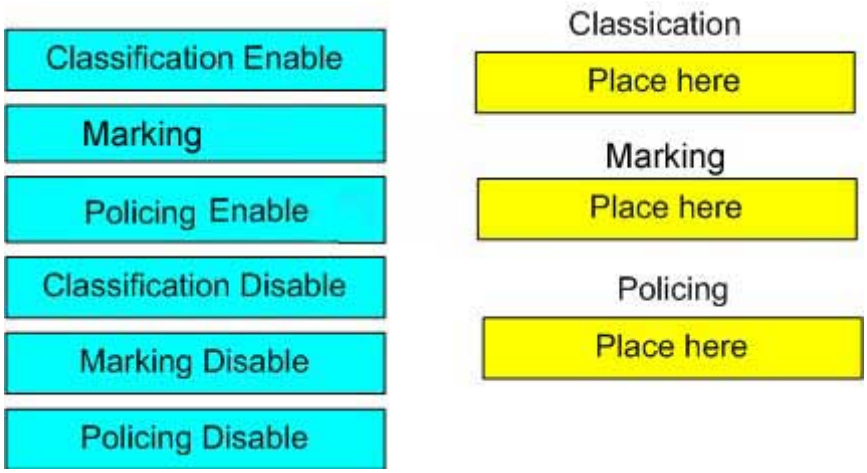
QUESTION 294
In an unmanaged CE router implementation, how does the service provider enforce the SLA?

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

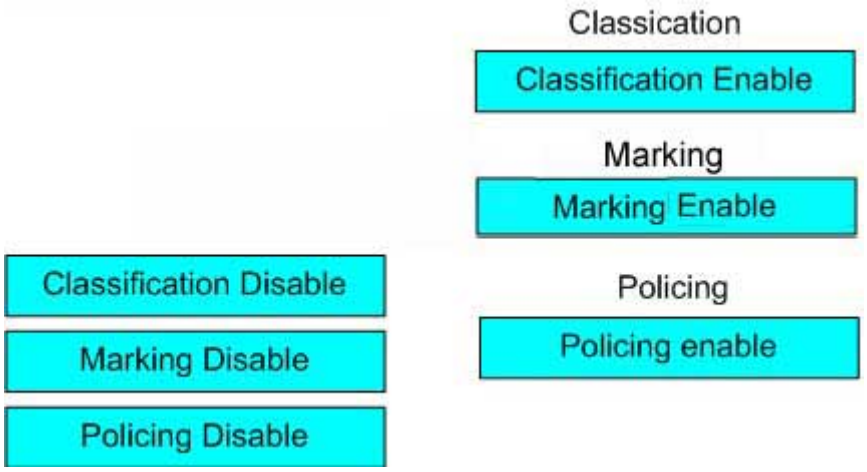
Answer: A

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 295
DRAG DROP
According to the best practices, identify the QoS mechanism that should applied at the inbound direction on the PE router's CE to PE link when using an unmanaged CE services by dragging and dropping the proper enable or disable state to the right.



Answer:



QUESTION 296
Exhibit:

```
class-map class-1
match ip rtp 2024 1000
class-map class 2
match dscp 5 6 7
policy-map access-group-1-traffic
class class-1
shape peak 16000
class class-2
police 8000 1000
conform-action set-dscp-transmit 1
exceed-action set-dscp-transmit 0
violate-action drop
class class-default
fair-queue 16
queue-limit 20
interface fastethernet 0/0
service-policy output access-group1-traffic
```

Refer to the exhibit. Which three statements are true about the configuration? (Choose three)

A. Traffic that is subject to shaping can burst up to 32,000 bps.
B. IP traffic (DSCPs 5, 6, and 7) that is sent on fastethernet 0/0 will be traffic policed.
C. RTP traffic (ports 2024 and 1000) that is sent on fastethernet 0/0 will be traffic shaped.
D. Traffic that is subject to policing will have the DCSP set to 0 if the rate exceeds 1000 bps.
E. IP traffic (DSCPs 1, 2, 3, and 4) that is sent on fastethernet 0/0 are considered to have a violate status and are dropped.
F. IP traffic (DSCP 0) that is sent on fastethernet 0/0 will be subject to fair queuing.

Answer: A, B, F

QUESTION 297
Which three factors will affect processing delay? (Choose three)

A. CPU speed
B. Router architecture
C. Queuing mechanism
D. Type of media
E. IP switching method
F. Distance of media

Answer: A, B, E

Explanation: There are lots delay but CPU Speed, Router Architecture and IP Switching method affects on Processing delay.

QUESTION 298
Which statement is true about the IntServ QoS model?

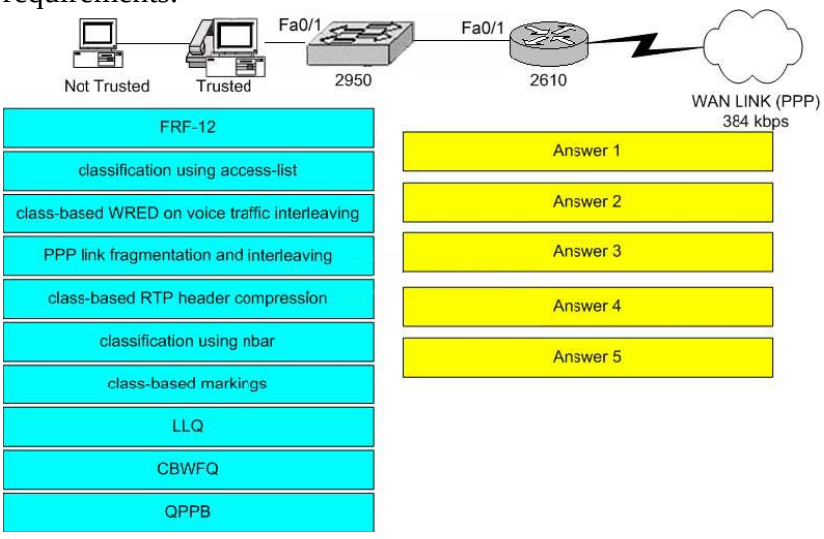
A. QoS traffic flows are managed on a hop-by-hop basis.
B. QoS traffic flows are guaranteed end-to-end.
C. QoS policies are not implemented, relying on best-effort delivery of packets.
D. QoS policies require that traffic be divided into classes.

Answer: B

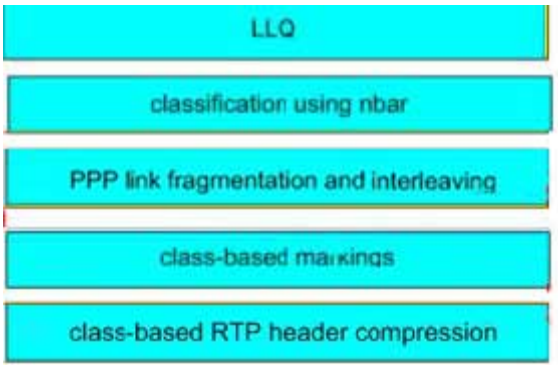
Explanation:
Integrated services (IntServ) is the name given to QoS signaling. QoS signaling allows an end station (or network node, such as a router) to communicate with its neighbors to request specific treatment for a given traffic type. This type of QoS allows for end-to-end QoS in the sense that the original end station can make a request for special treatment of its packets through the network, and that request is propagated through every hop in the

packet's path to the destination. True end-to-end QoS requires the participation of every networking device along the path (routers, switches, and so forth), and this can be accomplished with QoS signaling.
In 1994, RFC 1633 first defined the IntServ model. The following text, taken from RFC 1633, provides some insight as to the original intent of IntServ:
We conclude that there is an inescapable requirement for routers to be able to reserve resources, in order to provide special QoS for specific user packet streams, or "flows". This in turn requires flow-specific state in the routers, which represents an important and fundamental change to the Internet model.
As it turns out, the requirement was not as inescapable as the engineers who authored RFC 1633 originally thought, as evidenced by the fact that the Internet still relies almost entirely on BE delivery for packets.

QUESTION 299
DRAG DROP
Based on the topology shown, various applications traffic from the PC needs to be identified, classified, then marked as easily as possible. On the 2610 WAN link, voice traffic should have strict priority over all other traffic. Also ensure that the PC application traffic that have large payload does not cause excessive latency for the voice traffic and make the most efficient use of bandwidth on the WAN link. Drag the five appropriate QoS mechanisms into the boxed below 2610 to meet the given requirements.



Answer:



Explanation:
1- LLQ
as we got voice traffic, LLQ is the best answer. CBWFQ is not good for voice as is doesn't provide priority for voice
2- NBAR
since we got various application, then NBAR is the best to discover and classify them
3- MLP LFI
since speed of the link is less than 768 Kbps, we need fragmentation, either MLP LFI or FRF.12. FRF.12 doesn't support voice at all, so we choose MLP LFI
note FRF.11-Csupports voice
4- CB Marking
marking is usually used every where we use QoS, and it's the only marking choice that we got
5- RTP compression
RTP compression is one of the best solutions for voice transfer

---

QUESTION 300
Based on the following policy-map configuration, the bulk traffic class packets are not being ECN marked, yet there are many random drops in the bulk traffic class.
What is the most likely cause of the problem?

```
router(config)# policy-map MyPolicy
router(config-pmap)# class bulk
router(config-pmap)# bandwidth 128
router(config-pmap-c)# random-detect dscp-based
router(config-pmap-c)# random-detect dscp af31 32 40 10
router(config-pmap-c)# random-detect dscp af32 28 40 10
router(config-pmap-c)# random-detect dscp af33 24 40 10
router(config-pmap-c)# random-detect ecn
```

A. The CB-WRED min threshold is too low.
B. The CB-WRED max threshold is set too high.
C. The CB-WRED mark probability denominator is set too low.
D. The endpoints generating the bulk traffic packets are not ECN capable.
E. Some of the routers within the traffic path are not ECN capable.

Answer: D

Explanation:
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:
1. RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
2. Using IP precedence or DSCP value of the packets, packets with higher precedence are less likely to be dropped. If the default settings are preventing QoS, the precedence value can be used to control how WRED determines when and how often to drop packets.
3. The amount of bandwidth used by the traffic flow. Flows that use the most bandwidth are more likely to have packets dropped.
4. The weight factor defined for the interface determines how frequently packets are dropped.
WRED chooses the packets to drop after considering these factors in combination. The net result being that the highest priority and lowest bandwidth traffic is preserved.
WRED differs from standard random early detection (RED) in that RED ignores IP precedence, and instead drops packets from all traffic flows, not selecting low precedence or high bandwidth flows. By selectively dropping packets before congestion occurs, WRED prevents an interface from getting flooded, necessitating a large number of dropped packets. This increases the overall bandwidth usage for the interface.
An effective use of weighted random early detection is to avoid congestion on a predominantly TCP/IP network, one that has minimal UDP traffic and no significant traffic from other networking protocols. It is especially effective on core devices rather than edge devices, because the traffic marking performed on edge devices can then affect the WRED interfaces throughout the network. The disadvantage of WRED is that only predominantly TCP/IP networks can benefit. Other protocols, such as NetWare IPX/SPX, do not respond to dropped packets by lowering their transmission rates and just retransmit the packets at the same rate. WRED treats all non-TCP/IP packets as having precedence zero. In a mixed protocol environment, WRED might not be the best choice for queuing traffic.
Weighted random early detection interfaces automatically favor high priority, low bandwidth traffic flows. No specific policies are needed. However, because WRED automatically uses the IP precedence settings in packets, consider marking all traffic that enters the device or mark the traffic at the point where it enters the network. Marking all traffic will ensure that packets receive the service level intended.
To enable WRED on an interface use the command random-detect.
Router(config-if)#random-detect
No other commands or parameters need to be specified in order to configure WRED on the interface with the default parameter values.
The defaults can be changed with the following interface commands:

Router(config-if)#random-detect exponential-weighting-constant exponent min-threshold max-threshold mark-prob-denominator
This command configures the weight factor used in calculating the average queue length:
Router(config-if)#random-detect precedence precedence min-threshold max-threshold mark-prob-denominator
This command configures parameters for packets with a specific IP Precedence. The minimum threshold for IP Precedence zero corresponds to half the maximum threshold for the interface. The command must be issued for each precedence. To configure RED use the same parameters for each precedence. The default WRED parameter values are based on the best available data.

QUESTION 301
The following commands have been configured under the fa0/1 interface on the 2950 switch:
wrr-queue bandwidth 20180 0
mls qos trust cos
mls qos trust device cisco-phone
Voice traffic from the IP phone that is directly connected to the fa0/1 interface is experiencing excessive delays. What could be the cause of this problem?

A. The wrr-queue bandwidth weightings are not correct.
B. The default wrr-queue cos-map is being used.
C. The default cos-to-dscp map is being used.
D. The default dscp-to-cos map is being used.
E. The trust boundary configuration is not correct.

Answer: B

Explanation:
Use the wrr-queue bandwidth global configuration command to assign weighted round robin (WRR) weights to the four class of service (CoS) priority queues. Use the no form of this command to disable the WRR scheduler and enable the strict priority scheduler.
wrr-queue bandwidth weight1...weight4
no wrr-queue bandwidth
Use the show wrr-queue bandwidth user EXEC command to display the weighted round-robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

QUESTION 302
What does the following command accomplish?
router(config-pmap-c)# shape fecn-adapt

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

Answer: C

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 303
Which three characteristics are drawbacks to the use of a best-effort with over-provisioning backbone design? (Choose three)

A. The design costs more to implement than a DiffServ backbone.
B. Denial of Service attacks on one service can affect all network traffic.
C. The design uses a different over-provisioning ratio for the different traffic classes.
D. It requires complex QoS mechanisms at the network edge.
E. It requires complex QoS mechanisms at the network core.
F. Unplanned network failures can cause unexpected congestion in the network.

Answer: A, B, F

QUESTION 304
Which type of logical interface must be defined when configuring PPP multilink

LFI?

A. tunnel interface
B. Null0 interface
C. Multilink interface
D. Loopback interface
E. Virtual access interface
F. Dialer interface

Answer: C

Explanation:
The Cisco IOS Link Fragmentation and Interleaving (LFI) feature uses Multilink PPP (MLP). MLP provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.
Weighted fair queueing (WFQ) on MLP works at the packet level, not at the level of multilink fragments. Thus, if a small real-time packet gets queued behind a larger best-effort packet and no special queue has been reserved for real-time packets, the small packet will be scheduled for transmission only after all the fragments of the larger packet are scheduled for transmission.
WFQ is supported on all interfaces that support MLP, including MLP virtual access interfaces and virtual interface templates.
Fair queueing on MLP overcomes a prior restriction. Previously, fair queueing was not allowed on virtual access interfaces and virtual interface templates. Interleaving provides the delay bounds for delay-sensitive voice packets on a slow link that is used for other best-effort traffic.
To configure MLP and interleaving on a configured and operational interface or virtual

interface template, use the following commands in interface configuration mode:

Step	Command	Purpose
1.	**ppp multilink**	Enable MLP.
2.	**ppp multilink interleave**	Enable real-time packet interleaving.
3.	**ppp multilink fragment-delay** *milliseconds*	Optionally, configure a maximum fragment delay. If, for example, you want a voice stream to have a maximum bound on delay of 20 milliseconds (ms) and you specify 20 ms using this command, MLP will choose a fragment size based on the configured value.
4.	**ip rtp reserve** *lowest-UDP-port range-of-ports* [*maximum-bandwidth*]	Reserve a special queue for real-time packet flows to specified destination User Datagram Protocol (UDP) ports, allowing real-time traffic to have higher priority than other flows. If the bandwidth exceeds the limit specified, the reserved queue is degraded to a best-effort queue. (Use of this command is helpful in improving delay bounds of real-time traffic, such as voice streams, by giving them a higher priority.)
5.	multilink virtual-template	For virtual interface templates only, apply the virtual interface template to the multilink bundle

---

QUESTION 305
While using the "show auto qos" command, you notice that the QoS configuration generated by AutoQoS is not correct. What should you verify to troubleshoot this problem?

A. IP CEF configuration
B. Bandwidth configuration on the interfaces
C. Class-map configuration
D. NBAR configuration
E. Clock rate configuration on the interfaces
F. Policy-map configuration

Answer: B

Explanation:
The AutoQoS for the Enterprise feature automates the deployment of quality of service (QoS) policies in a general business environment, particularly for midsize companies and branch offices of larger companies. Existing QoS policies may be present during the first configuration phase of this feature, that is, during the Auto-Discovery (data collection) phase. However, any existing QoS policies must be removed before the AutoQoS-generated polices are applied during the second configuration phase of this feature.
show auto qos [interface [interface type]]

If you got the error generated while configuring Auto QoS you need to specify the bandwidth:
Example:
Router> enableRouter# configure terminalRouter(config)#interface s4/0
Router(config-if)#bandwidth 1540Router(config-if)#auto discovery qos
Router(config-if)#exit

QUESTION 306
Which policy-map configuration, when applied to an interface in the output direction, will always rate-limit the kazaa1 traffic to 8000 bps going out on the interface even when there is no congestion on the interface?

A. class-map p2p
match protocol kazaa2
policy-map limitp2p
class p2p
bandwidth 8
B. class-map p2p
match protocol kazaa2
policy-map limitp2p
class p2p
police 8000 conform-action transmit exceed-action drop

Answer: B

Explanation:
Router(config-pmap-c)#policebps burst-normal burst-maxconform-action action exceed-action action violate-action action : Specifies a maximum bandwidth usage by a traffic class.The police command polices traffic based on a token bucket algorithm. The variables in the token bucket algorithm are set in this command line.

QUESTION 307
Which QoS mechanism calculates the mean queue depth to determine its operation?

A. WRED
B. LLQ/CBWFQ
C. WFQ
D. Class-based shaping
E. Class-based policing

Answer: A

Explanation:
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:
1. RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
2. Using IP precedence or DSCP value of the packets, packets with higher precedence are less likely to be dropped. If the default settings are preventing QoS, the precedence value can be used to control how WRED determines when and how often to drop packets.
3. The amount of bandwidth used by the traffic flow. Flows that use the most bandwidth are more likely to have packets dropped.
4. The weight factor defined for the interface determines how frequently packets are dropped.
WRED chooses the packets to drop after considering these factors in combination. The net result being that the highest priority and lowest bandwidth traffic is preserved.
WRED differs from standard random early detection (RED) in that RED ignores IP precedence, and instead drops packets from all traffic flows, not selecting low precedence or high bandwidth flows. By selectively dropping packets before congestion occurs, WRED prevents an interface from getting flooded, necessitating a large number of dropped packets. This increases the overall bandwidth usage for the interface.
An effective use of weighted random early detection is to avoid congestion on a predominantly TCP/IP network, one that has minimal UDP traffic and no significant traffic from other networking protocols. It is especially effective on core devices rather than edge devices, because the traffic marking performed on edge devices can then affect the WRED interfaces throughout the network. The disadvantage of WRED is that only predominantly TCP/IP networks can benefit. Other protocols, such as NetWare IPX/SPX, do not respond to dropped packets by lowering their transmission rates and just retransmit the packets at the same rate. WRED treats all non-TCP/IP packets as having precedence zero. In a mixed protocol environment, WRED might not be the best choice for queuing traffic.
Weighted random early detection interfaces automatically favor high priority, low bandwidth traffic flows. No specific policies are needed. However, because WRED automatically uses the IP precedence settings in packets, consider marking all traffic that enters the device or mark the traffic at the point where it enters the network. Marking all traffic will ensure that packets receive the service level intended.

QUESTION 308
What will be the peak shape rate based on the configuration that follows?
policy-map setpeak
class all-traffic
shape peak 32000

A. 16000 bps
B. 32000 bps

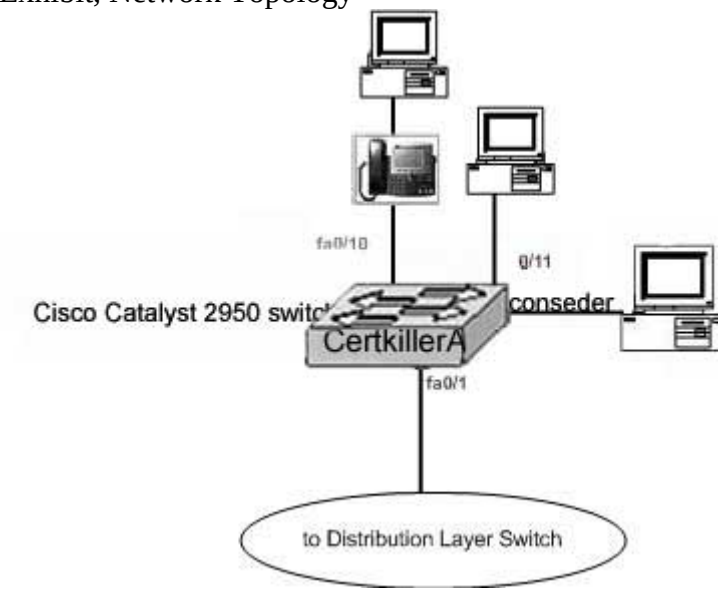
C. 48000 bps
D. 64000 bps
E. 80000 bps
F. 96000 bps

Answer: D

Explanation:
Traffic shaping allows you to control the traffic going out an interface in order to match its transmission to the speed of the remote, target interface and to ensure that the traffic conforms to policies contracted for it. Traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.
Using the Class-Based Shaping feature, you can do the following:
Configure generic traffic shaping (GTS) on a traffic class
Specify average rate or peak rate traffic shaping
Configure class-based weighted fair queueing (CBWFQ) inside GTS
Class-based shaping can be enabled on any interface that supports GTS.
Configuring GTS on a Traffic Class
Using the Class-Based Shaping feature, you can configure GTS on a class, rather than only on an access control list (ACL). In order to do so, you must first define traffic classes based on match criteria including protocols, ACLs, and input interfaces. You can then apply traffic shaping to each defined class.
Specifying Average Rate or Peak Rate Traffic Shaping
Traffic shaping limits the rate of transmission of data. In addition to using a specifically configured transmission rate, you can use GTS to specify a derived transmission rate based on the level of congestion.
You can specify two types of traffic shaping; average rate shaping and peak rate shaping. Average rate shaping limits the transmission rate to the committed information rate (CIR). Using the CIR ensures that the average amount of traffic being sent conforms to the rate expected by the network.
Peak rate shaping configures the router to send more traffic than the CIR. To determine the peak rate, the router uses the following formula:
peak rate = CIR(1+Be/Bc)
where:
Be is the Excess Burst rate.
Bc is the Committed Burst rate.
Peak rate shaping allows the router to burst higher than average rate shaping. However, using peak rate shaping, the traffic sent above the CIR (the delta) has the potential of being dropped if the network becomes congested.
If your network has additional bandwidth available (over the provisioned CIR) and the application or class can tolerate occasional packet loss, that extra bandwidth can be exploited through the use of peak rate shaping. However, there may be occasional packet drops when network congestion occurs. If the traffic being sent to the network must strictly conform to the configured network provisioned CIR, then you should use average traffic shaping.

Configuring CBWFQ Inside GTS
Prior to this release, when GTS queues packets that, when sent, cause the traffic flow to violate the configured rate, only flow-based WFQ was supported for the queued packets. Using the Class-Based Shaping feature, CBWFQ is supported for the queued packets. You can use CBWQ to configure classes of queued traffic and provide relative or absolute bandwidth guarantees to those classes. Note that the relative or absolute bandwidth guarantees are with regard to the configured CIR.

QUESTION 309
SIMULATION
Exhibit, Network Topology

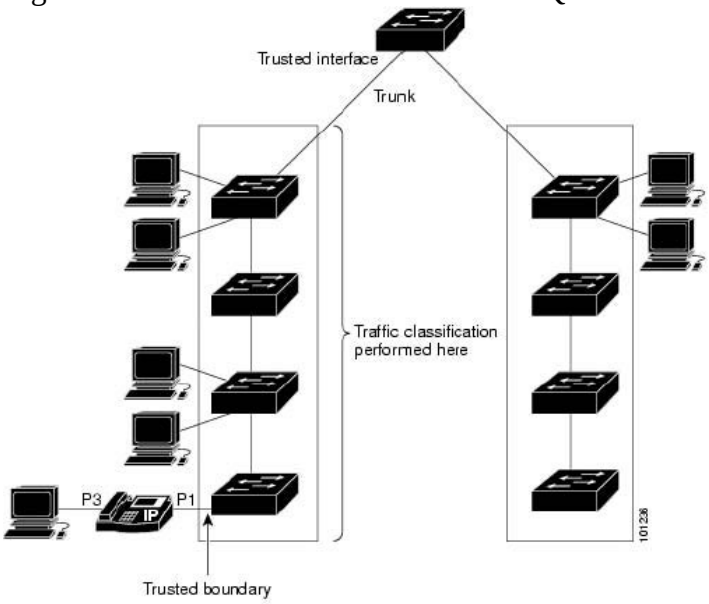


You work as a network technician at Certkiller .com. You are required to configure the fa0/1, fa0/10 and fa0/11 ports on the Cisco Catalyst 2950 switch according to the following:
On port fa0/1, trust all incoming DSCP settings.
On port fa0/1, trust all incoming CoS settings.
On port fa0/10, trust the incoming CoS setting only if a Cisco IP Phone is connected to the fa0/10 port: otherwise do not trust any CoS or DSCP markings coming in.

Answer:

Explanation:
Certkiller A(config)#cdp enable
Certkiller A(config)#interface fastethernet0/1
Certkiller A(config-if)#mls qos trust dscp
Certkiller A(config-if)#interface fastethernet0/11 ----------assume this must be fa0/11 question has misprint
Certkiller A(config-if)#mls qos trust cos
Certkiller A(config-if)#interface fastethernet0/10
Certkiller A(config-if)#mls qos trust device cisco-phone
Certkiller A(config-if)#end

Certkiller A#show mls qos interface fastethernet0/1
Certkiller A#show mls qos interface fastethernet0/11
Certkiller A#show mls qos interface fastethernet0/10
Certkiller A#copy running-config startup-config
This weblink seems to support this:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2940/12122ea2/2940scg/swqos.htm
Configuring the Trust State on Ports within the QoS Domain
Packets entering a QoS domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the QoS domain.
Figure24-2 Port Trusted States within the QoS Domain



Beginning in privileged EXEC mode, follow these steps to configure the port to trust the classification of the traffic that it receives:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to be trusted, and enter interface configuration mode. Valid interfaces include physical interfaces.
Step 3	**mls qos trust** [**cos**]	Configure the port trust state. 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. For more information about this command, see the command reference for this release.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show mls qos interface** [*interface-id*]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring the CoS Value for an Interface

QoS assigns the CoS value specified with the mls qos cos interface configuration command to untagged frames received on trusted and untrusted ports.

Beginning in privileged EXEC mode, follow these steps to define the default CoS value of a port or to assign the default CoS to all incoming packets on the port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to be trusted, and enter interface configuration mode. Valid interfaces include physical interfaces.
Step 3	**mls qos trust** [**cos**]	Configure the port trust state. 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. For more information about this command, see the command reference for this release.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show mls qos interface** [*interface-id*]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Trusted Boundary

In a typical network, you connect a Cisco IP Phone to a switch port as shown in Figure24-2. 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.

Beginning in privileged EXEC mode, follow these steps to configure trusted boundary on a switch port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp enable**	Enable CDP globally. By default, it is enabled.
Step 3	**interface** *interface-id*	Specify the interface to be trusted, and enter interface configuration mode. Valid interfaces include physical interfaces.
Step 4	**cdp enable**	Enable CDP on the interface. By default, CDP is enabled.
Step 5	**mls qos trust device cisco-phone**	Configure the Cisco IP Phone as a trusted device on the interface.
Step 6	**mls qos trust cos**	Configure the port trust state to trust the CoS value of the ingress packet. By default, the port is not trusted.For more information on this command, see the command reference for this release.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show mls qos interface** [*interface-id*]	Verify your entries.
Step 9	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

Enabling Pass-Through Mode

When the switch is in pass-through mode, it uses the CoS value of incoming packets without modifying the DSCP value and sends the packets from one of the four egress queues. By default, pass-through mode is disabled. The switch assigns a CoS value of 0 to all incoming packets without modifying the packets. The switch offers best-effort service to each packet regardless of the packet contents or size and sends it from a single egress queue.

Beginning in privileged EXEC mode, follow these steps to enable pass-through mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which pass-through mode is enabled, and enter interface configuration mode. Valid interfaces include physical interfaces.
Step 3	**mls qos trust cos pass-through dscp**	Enable pass-through mode. The interface is configured to trust the CoS value of the incoming packets and to send them without modifying the DSCP value.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show mls qos interface** [*interface-id*]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable pass-through mode, use the no mls qos trust pass-through dscp interface configuration command.
If you enter the mls qos cos override and the mls qos trust [cos] interface commands when pass-through mode is enabled, pass-through mode is disabled.
If you enter the mls qos trust cos pass-through dscp interface configuration command when the mls qos cos override and the mls qos trust [cos] interface commands are already configured, pass-through mode is disabled.

QUESTION 310

```
Certkiller3 #show class-map
Class | Map match-any class-default    (id 0)
  Match any
Class Map match-all financeA (id 1)
  Match protocol ip
  Match qos-group 2
Class Map match-any financeZ (id 2)
  Match class-map financeA
  Match input-interface Ethernet0/0
  Match dscp af11
Certkiller3 #show policy-map
 Policy Map finance
   Class financeZ
    police cir 1000000 bc 500000 be 500000
      conform-action transmit
      exceed-action set-frde-transmit
```

Refer to the exhibit, Which traffic will have Frame Relay DE bit set when transmitted out the interface or interfaces that the policy-map is assigned to, assuming that CIR has been exceeded?

A. IP packets assigned to qos-group 2
B. IP packets with any DSCP setting

C. IP packets exiting the Ethernet0/0 interface
D. Class-default traffic
E. All traffic

Answer: A

Explanation:
The show policy-map command displays the configuration of a service policy map created using the policy-map command. You can use the show policy-map command to display all class configurations comprising any existing service policy map, whether or not that service policy map has been attached to an interface.
You can use the show class-map command to display all class maps and their matching criteria. If you enter the optional class-map-name argument, the specified class map and its matching criteria will be displayed.
Examples
In the following example, three class maps are defined. Packets that match access list 103 belong to class c3, IP packets belong to class c2, and packets that come through input interface Ethernet1/0 belong to class c1. The output from the show class-map command shows the three defined class maps.
Router# show class-map
Class Map c3
Match access-group 103
Class Map c2
Match protocol ip
Class Map c1
Match input-interface Ethernet1/0

QUESTION 311
Which four of the following bit values are used for bits 5-7 of the DSCP field to select AF PHB? (Choose four.)

A. 000
B. 001
C. 010
D. 011
E. 100
F. 101

Answer: B, C, D, E

Explanation:
Assured Forwarding
RFC 2597 defines the assured forwarding (AF) PHB and describes it as a means for a provider DS domain to offer different levels of forwarding assurances for IP packets received from a customer DS domain. The Assured Forwarding PHB guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available.

There are four AF classes, AF1x through AF4x. Within each class, there are three drop probabilities. Depending on a given network's policy, packets can be selected for a PHB based on required throughput, delay, jitter, loss or according to priority of access to network services.
Classes 1 to 4 are referred to as AF classes. The following table illustrates the DSCP coding for specifying the AF class with the probability. Bits DS5, DS4 and DS3 define the class; bits DS2 and DS1 specify the drop probability; bit DS0 is always zero.

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medium	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
High	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

QUESTION 312
Which QoS mechanism adds IP Precedence information for prefixes into the FIB table?

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

Answer: C

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 313
Based on the following 2950 switch configuration, 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 1 is setup as the expedite queue.

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

Answer: E

Explanation:
In brief, the Catalyst 2950 Family of switches supports the following output scheduling mechanism:
1. Strict-priority scheduling
2. WRR scheduling
Strict-priority scheduling services packets placed into higher-priority queues before servicing packets in lower-priority queues. Although this mechanism works well for high-priority traffic such as Voice over IP (VoIP), this mechanism may starve transmission of traffic in lower-priority queues. As a result, the second option of using WRR scheduling exists. WRR transmits traffic based on a weight value. In this manner, each queue receives an assigned weight of the total bandwidth. Therefore, during any period of time, the switch sends traffic out of every queue based on its weighted value. Subsequent sections discuss these mechanisms in more detail with configuration examples.
In brief, the Catalyst 3550 Family of switches supports the following queuing and output scheduling mechanisms:
Expedite (strict-priority) queue WRR scheduling Configurable drop thresholds per output queue WRED congestion avoidance algorithm The Catalyst 3550 Family of switches uses WRR scheduling for output scheduling in a manner similar to the Catalyst 2950 Family of switches. However, the Catalyst 3550 Family of switches allows for designation of an expedite queue and configuration of congestion avoidance mechanisms using tail-drop thresholds or WRED. The designation of the expedite queue forces strict priority of transmission on the respective egress queue. The congestion avoidance algorithms attempt to subside congestion by dropping packets with lower priority before higher-priority packets in the same transmit queue. Later sections of this chapter discuss these features in more detail.
User Configuring and Verifying the DSCP-to Transmit Queue Mapping Table
Switch#configure terminal
Switch(config)#wrr-queue cos-map 1 0 1 2
Switch(config)#wrr-queue cos-map 2 3 4
Switch(config)#wrr-queue cos-map 3 5
Switch(config)#end
Switch#show wrr-queue cos-map
CoS Value : 0 1 2 3 4 5 6 7
Priority Queue : 1 1 1 2 2 3 4 4

QUESTION 314
Which show command is used to examine class-based WRED drop statistics?

A. show queue {interface}
B. show queueing
C. show queueing random-detect
D. show interface
E. show interface random-detect
F. show policy-map interface {interface}

Answer: F

Explanation:
To display the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface, use the show policy-map interface command in EXEC mode.

QUESTION 315
Which parameter must be set to a value greater than 0 to enable traffic shaping to temporarily burst above the committed rate?

A. Bc
B. Be
C. CIR
D. PIR
E. MinCIR
F. Tc

Answer: B

Explanation:
Traffic shaping allows you to control the traffic going out 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 contracted for it. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.
Traffic Shaping and Rate of TransferTraffic shaping limits the rate of transmission of data. You can limit the data transfer to one of the following:
1. A specific configured rate
2. A derived rate based on the level of congestion
As mentioned, the rate of transfer depends on these three components that constitute the token bucket: burst size, mean rate, measurement (time) interval. The mean rate is equal to the burst size divided by the interval.
When traffic shaping is enabled, the bit rate of the interface will not exceed the mean rate over any integral multiple of the interval. In other words, during every interval, a maximum of burst size can be sent. Within the interval, however, the bit rate may be faster than the mean rate at any given time.
One additional variable applies to traffic shaping: Be size. The Excess Burst size corresponds to the number of noncommitted bits-those outside the committed

information rate (CIR)-that are still accepted by the Frame Relay switch but marked as discard eligible.
In other words, the Be size allows more than the burst size to be sent during a time interval in certain situations. The switch will allow the packets belonging to the Excess Burst to go through but it will mark them by setting the discard eligible (DE) bit. Whether the packets are sent depends on how the switch is configured.
When the Be size equals 0, the interface sends no more than the burst size every interval, achieving an average rate no higher than the mean rate. However, when the Be size is greater than 0, the interface can send as many as Bc+Be bits in a burst, if in a previous time period the maximum amount was not sent. Whenever less than the burst size is sent during an interval, the remaining number of bits, up to the Excess Burst size, can be used to send more than the burst size in a later interval.

QUESTION 316
Which algorithm (discard method) does WRED use to determine which packets will be dropped when the average queue length becomes larger than the user-specified maximum threshold?

A. tail discard
B. random discard
C. weighted early discard
D. packet size based discard

Answer: A

Explanation:
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:
1. RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
2. Using IP precedence or DSCP value of the packets, packets with higher precedence are less likely to be dropped. If the default settings are preventing QoS, the precedence value can be used to control how WRED determines when and how often to drop packets.
3. The amount of bandwidth used by the traffic flow. Flows that use the most bandwidth are more likely to have packets dropped.
4. The weight factor defined for the interface determines how frequently packets are dropped.
WRED chooses the packets to drop after considering these factors in combination. The net result being that the highest priority and lowest bandwidth traffic is preserved. WRED differs from standard random early detection (RED) in that RED ignores IP precedence, and instead drops packets from all traffic flows, not selecting low precedence or high bandwidth flows. By selectively

dropping packets before congestion occurs, WRED prevents an interface from getting flooded, necessitating a large number of dropped packets. This increases the overall bandwidth usage for the interface.
An effective use of weighted random early detection is to avoid congestion on a predominantly TCP/IP network, one that has minimal UDP traffic and no significant traffic from other networking protocols. It is especially effective on core devices rather than edge devices, because the traffic marking performed on edge devices can then affect the WRED interfaces throughout the network. The disadvantage of WRED is that only predominantly TCP/IP networks can benefit. Other protocols, such as NetWare IPX/SPX, do not respond to dropped packets by lowering their transmission rates and just retransmit the packets at the same rate. WRED treats all non-TCP/IP packets as having precedence zero. In a mixed protocol environment, WRED might not be the best choice for queuing traffic.
Weighted random early detection interfaces automatically favor high priority, low bandwidth traffic flows. No specific policies are needed. However, because WRED automatically uses the IP precedence settings in packets, consider marking all traffic that enters the device or mark the traffic at the point where it enters the network. Marking all traffic will ensure that packets receive the service level intended

---

QUESTION 317
QoS policy propagation through BGP (QPPB) supports which two QoS markers? (Choose two.)

A. DSCP
B. IP precedence
C. QoS group
D. COS
E. MPLS EXP

Answer: B, C

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.
1. QPPB uses BGP attributes to advertise CoS to other Routers in the network
2. BGP communities are usually used to propagate CoS information bound to IP networks.
3. Packet classification policy can be propagated via BGP without having to use complex access lists at each of a large number of border routers.
4. A route map is used to translate BGP information (For example BGP community Value) into IP precedence or QoS group
5. QPPB can only classify and mark inbound packets.

QUESTION 318
What does the term serialization delay refer to?

A. a fixed delay referring to the time it takes for a frame to transit the physical media
B. a fixed delay referring o the time it takes to encode bits of packets onto the physical interface
C. a variable delay caused by packet loss across a congested serial WAN link
D. a variable delay caused by the processing tasks of a network device, such as route lookup, header changes, and switching

Answer: B

Explanation:
Serialization is the process of placing bits on the circuit. The higher the circuit speed, the less time it takes to place the bits on the circuit. Therefore, the higher the speed of the link, the less serialization delay is incurred.

QUESTION 319
What is the purpose of the ip nbar port-map command?

A. configures stateful NBAR to recognize applications based on dynamic port numbers
B. configures NBAR to search for a particular protocol using a port number other than the well-known port number
C. configure NBAR to recognize non-TCP and non-UDP applications
D. configure NBAR for subport classifications (like HTTP URLs or MIME)
E. configures NBAR to recognize applications that use FastTrack (like Kazaa, and Morpheus)

Answer: B

Explanation:
To configure Network-Based Application Recognition (NBAR) to search for a protocol or protocol name using a port number other than the well-known port, use the ip nbar port-map global configuration command. To look for the protocol name using only the well-known port number, use the no form of this command.
ip nbar port-map protocol-name [tcp | udp] port-number
no ip nbar port-map protocol-name [tcp | udp] port-number

QUESTION 320
This policy-map is applied to a 128-kbps serial interface in the output direction.
Which set of additional commands within this policy-map will improve the link efficiency on the serial interface?
policy-map test
class voice
priority 25
class telnet

bandwidth remaining percent 20
class ftp
bandwidth remaining percent 30

A. class voice
no priority 25
bandwidth percent remaining 25
B. class voice
compression header ip tcp
C. class telnet
compression header ip tcp
D. class telnet
fair-queue
E. class ftp
fair-queue
F. class ftp
compression header up

Answer: C

Explanation:
RTP and TCP IP Header Compression
RTP or TCP IP header compression is a mechanism that compresses the IP header in a data packet before the packet is transmitted. Header compression reduces network overhead and speeds up transmission of RTP and TCP packets.
Cisco IOS software provides a related feature called Express RTP/TCP Header Compression. Before this feature was available, if compression of TCP or RTP headers was enabled, compression was performed in the process-switching path. Compression performed in this manner meant that packets traversing interfaces that had TCP or RTP header compression enabled were queued and passed up the process to be switched. This procedure slowed down transmission of the packet, and therefore some users preferred to fast-switch uncompressed TCP and RTP packets.
Now, if TCP or RTP header compression is enabled, it occurs by default in the fast-switched path or the Cisco Express Forwarding-switched (CEF-switched) path, depending on which switching method is enabled on the interface. Furthermore, the number of TCP and RTP header compression connections was increased.
If neither fast-switching nor CEF-switching is enabled, then if TCP or RTP header compression is enabled, it will occur in the process-switched path as before.
The Express RTP and TCP Header Compression feature has the following benefits:
It reduces network overhead.
It speeds up transmission of TCP and RTP packets. The faster speed provides a greater benefit on slower links than faster links.
SUMMARY STEPS
1. enable
2. configure {terminal | memory | network}
3. policy-map policy-name

4. class-map class-map-name
5. compression header ip {rtp | tcp}
6. exit

QUESTION 321
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. 40 bps
C. 150 bps
D. 240 bps
E. 480 bps
F. 640 bps

Answer: C

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 322
Which two different traffic types have the most similar sensitivity to latency, jitter, and packet loss? (Choose two.)

A. SQL transactions
B. Voice
C. Voice signaling
D. Streaming video
E. Video conferencing
F. Peer-to-peer file sharing

Answer: B, E

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 323
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 voice traffic class is missing the random-detect command.
C. The mission-critical traffic class bandwidth guarantee should be lower than the voice traffic class priority bandwidth guarantee.
D. The mission-critical traffic class is mission the queue-limit command.
E. Fair-queue should be enabled for the mission-critical traffic class.

Answer: A

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 324
Which two commands are typically applied to the voice traffic class within a policy-map? (Choose two.)

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

Answer: B, D

Explanation:
1. 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.
2. 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.

QUESTION 325
In which two locations is the qos pre-classify command applied to support QoS preclassification over an IPSec/GRE tunnel? (Choose two.)

A. the tunnel interface
B. the physical interface
C. the crypto map
D. the policy-map
E. the class-map

Answer: A, C

Explanation:
Configuring QoS for VPNs
The QoS for VPNs feature, which is enabled by the qos pre-classify command, is restricted to tunnel and virtual template interfaces, and crypto map configuration submodes. For generic routing encapsulation(GRE) and IP in IP(IPIP) tunnel protocols, the qos pre-classify command is applied on the tunnel interface, making QoS for VPNs a configuration option on a per-tunnel basis.
For Layer 2 Forwarding(L2F) and Layer 2 Tunneling Protocol(L2TP) protocols, the qos pre-classify command is applied on the virtual template interface. L2TP clients belonging to identical virtual private dial-up network (VPDN) groups inherit the preclassification setting. The qos pre-classify command can be configured on a per-VPDN tunnel basis.
For IPSec tunnels, the qos pre-classify command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption.
The following example enables the QoS for Virtual Private Networks (VPNs) feature on tunnel interfaces and virtual templates:
Router(config-if)# qos pre-classifyThe following example enables the QoS for VPNs feature on crypto maps:
Router(config-crypto-map)# qos pre-classify

QUESTION 326
What is the purpose of using multiactions traffic policing?

A. so that exceed traffic can be shaped and violate traffic can be policed
B. so that conform, exceed, and violate traffic can be marked with different CLPs
C. so that conform traffic from different flows can be marked with different DSCPs
D. so that class-based policing can mark at Layer 2 and Layer 3 at the same time
E. so that traffic can be policed using two separate rates

Answer: D

Explanation:
Multiactions traffic policing helps to class-based policing can mark at Layer 2 and Layer 3 at the same time.

QUESTION 327
Switch port fa0/2 has been configured to connect an IP phone with an attached PC. Given the set of commands shown below, where does the trust boundary lie?
interface fa0/2
mls qos trust cos
mls qos trust device cisco-phone
switchport voice vlan 112

A. between the IP phone and the switch
B. between the IP phone and the PC
C. between the access layer switch and the distribution layer switch
D. between the PC port and the LAN port on the IP phone

Answer: A

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 328
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. WRR, FRTS, FRF.12, and CB-RTP header compression
B. WRR, CB-WRED, CB-Marking, FRF.12, and CB-RTP header compression
C. CBWFQ, CB-WRED, CB-Marking, CB-Policing, and FRTS
D. CBWFQ, FRTS, FRF.12, and CB-RTP header compression
E. LLQ, CB-WRED, CB-Marking, FRTS, FRF.12, and CB-RTP header compression
F. LLQ, CB-WRED, CB-Policing, and CB-TCP and CB-RTP header compressions

Answer: E

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 prioritybw
Router(config-pmap)#class class-default fair-queue
Router(config-pmap-c)#class priorityтraffic 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 329
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. Use TCP header compression and LFI to reduce delays.
B. Prioritize voice traffic as the highest priority to ensure that voice traffic is always serviced by the priority queue.
C. Use advanced technologies to compress all video and graphics traffic on the network.
D. Use class-based weighted fair queuing to prioritize voice traffic with a higher weight than all other traffic.

Answer: B

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 330
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. Traffic policing should be implemented to rate-limit the ingress traffic into the P router.
B. 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.
C. 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.
D. 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.

Answer: B

QUESTION 331
Exhibit:

```
sf#show ip nbar protocol-discovery

 FastEthernet0/0
                          Input                     Output
   Protocol               Packet Count              Packet Count
                          Byte Count                Byte Count
                          5 minute bit rate (bps)   5 minute bit rate (bps)
   ------------------------------------------------------------------------
   http                   25423                     17684
                          9750389                   3322284
                          121000                    41000
   sqlnet                 44837                     30061
                          5181115                   3199252
                          64000                     40000
   netbios                20203                     19787
                          2522278                   2398417
                          31000                     30000

   <output omitted>

   unknown                193288                    112278
                          14486461                  11798722
                          175000                    143000
   Total                  392763                    322755
                          49135566                  32567005
                          600000                    398000
```

Refer to the exhibit. According to the show output, which statement is true?

A. NBAR protocol discovery has been enabled on the router through the use of the match protocol commands within the class-map.
B. The unknown protocol traffic statistics refer to all the traffic matched by the class-default traffic class.
C. HTTP is the most active protocol on the Fa0/0 interface based on byte count.
D. The 5-minute average bits-per-second rate for all traffic entering the Fa0/0 interface is 398 kbps.
E. There is a total of 39,990 NetBIOS packets exiting the Fa0/0 interface.

Answer: C

Explanation:
The first step in being able to classify network traffic is to actually know what protocols

and applications are running on the network. This knowledge enables administrators to prioritize business-critical information and applications over less-important applications. Unfortunately, to configure ACLs to classify network traffic you must have prior knowledge of the network applications, as well as their associated protocol or port numbers. One option for discovering the protocols currently traversing an interface within the network is using NBAR protocol discovery.
NBAR is capable of recognizing any protocol included within the PDLM file. Protocol discovery is applied to the desired interface or group of interfaces using the following command at each intended interface:
ip nbar protocol-discovery
When protocol discovery is applied to the interface, statistics are gathered depicting the active protocols traversing the interface. To view the results of the protocol discovery process, use the following command:
show ip nbar protocol-discovery [interface type num]

QUESTION 332
Which command is needed to correct the following configurations in order to enable ppp multilink LFI on the s0/0 interface?
interface Serial0/0
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
no fair-queue
ppp multilink
multilink-group 2001100114
!
interface Multilink2001100114
bandwidth 384
ip address 10.1.1.1 255.255.255.0
service-policy output AutoQoS-Policy-UnTrust
ppp multilink
ppp multilink fragment-delay 10
ppp multilink interleave

A. the no ip address command on the s0/0 interface
B. the multilink-group 2001100114 command on the Multilink2001100114 interface
C. the ppp multilink load-threshold command on the s0/0 interface
D. the ppp multilink load-threshold command on the Multilink2001100114 interface
E. the ppp multilink interleave command on the s0/0 interface

Answer: A

Explanation:
You need to remove the IP Address of Physical Interface using no ip address command.

QUESTION 333
A Cisco Catalyst switch has an IP phone connected to its Fastethernet0/2 port. The

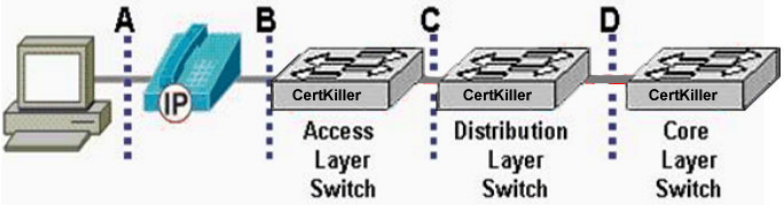
IP phone has an attached PC. The Fastethernet0/2 port on the switch has been configured with the commands mls qos trust cos, mls qos trust device cisco-phone, and switchport priority extend trust. What will happen to a data frame with a CoS of 5 that is sent from the PC through the IP phone to port Fastethernet0/2 on the switch?

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

Answer: B

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 334
Exhibit:



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. A
B. B
C. C
D. D

Answer: B

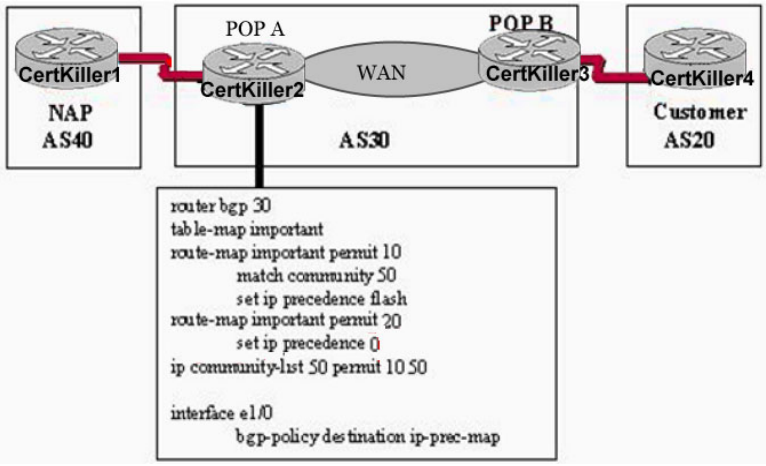
Explanation:
In a typical network, you connect a Cisco IP Phone to a switch port. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For 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 335
Which three characteristics best describe a converged network? (Choose three.)

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

Answer: C, D, F

QUESTION 336
Exhibit:



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?

A. Traffic from AS20 must have the community attribute set to 10:50 in a route-map, and send-community must be specified.
B. No actions are needed. Traffic must be marked in AS20 by the customer as 10:50 before it arrives at the service provider.
C. 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.
D. Traffic from AS20 must be automatically marked via an inbound QoS map on POP B, resulting in the community attribute set to 10:50.

Answer: A

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.
1. QPPB uses BGP attributes to advertise CoS to other Routers
2. BGP communities are usually used to propagate CoS information bound to IP networks
3. Packet classification policy can be propagated via BGP without having to use complex access lists at each of a large number of border routers
4. A route map is used to translate BGP information into IP precendence or QoS roup
5. QPPB can only classify and mark inbound packets

6. Propagate the CoS by encoding it into BGP attributes
7. 1. BGP Communities
2. AS Paths
3. IP prefixes
4. Any other BGP attribute
5. Translate the selected BGP attribute into either:
6. 1. IP Precedence
2. QoS group
3. Enable CEF and packet marking on interfaces

- 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 #>
```

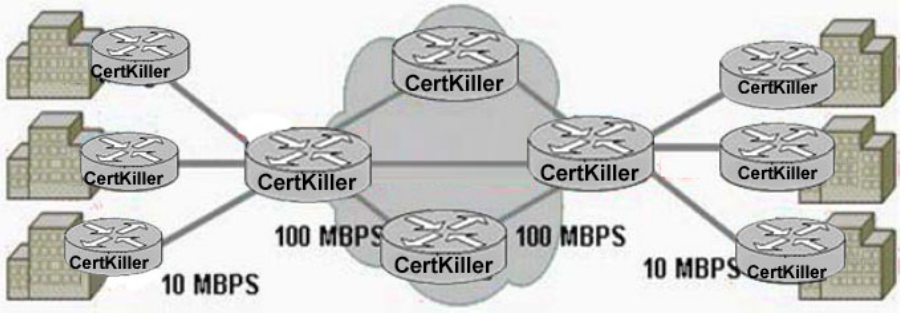
- Apply the route map to BGP routes that are in the BGP table. The **table-map** command is used to accomplish this task as follows:

```
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 337
Exhibit:



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

Answer: B

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

QUESTION 338
Where is the fragment size configured when using FRF.12 link fragmentation and interleaving?

A. within the physical serial interface
B. within the Frame Relay map-class
C. within the MQC policy-map
D. within the MQC class-map
E. within the MQC service-policy
F. within the logical multilink interface

Answer: B

Explanation:
The purpose of end-to-end FRF.12 fragmentation is to support real-time and non-real-time data packets on lower-speed links without causing excessive delay to the real-time data. FRF.12 fragmentation is defined by the FRF.12 Implementation Agreement. This standard was developed to allow long data frames to be fragmented into smaller pieces (fragments) and interleaved with real-time frames. In this way, real-time and non-real-time data frames can be carried together on lower-speed links without causing excessive delay to the real-time traffic.
End-to-end FRF.12 fragmentation is recommended for use on permanent virtual circuits (PVCs) that share links with other PVCs that are transporting voice and on PVCs transporting Voice over IP (VoIP). Although VoIP packets should not be fragmented, they can be interleaved with fragmented packets.
To configure the map class to support FRF.12 fragmentation, use the following map-class configuration command:

Command	Purpose
Router(config-map-class)# **frame-relay fragment** *fragment_size*	Configures Frame Relay fragmentation for the map class. The *fragment_size* argument defines the payload size of a fragment; it excludes the Frame Relay headers and any Frame Relay fragmentation header. The valid range is from 16 to 1600 bytes, and the default is 53. The value of *fragment_size* should be less than or equal to the MTU size. Set the fragmentation size such that the largest data packet is not larger than any voice packets.

QUESTION 339
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. DSCP markings from the Cisco IP Phone are trusted.

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

Answer: B

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 340
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 extend [cos value]
B. no mls qos trust dscp
C. mls qos trust cos
D. mls qos trust device cisco-phone
E. switchport priority extend trust
F. mls qos cos 5

Answer: C, D

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 341
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. CBWFQ and CB-WRED should be implemented on the P router egress to provide a maximum bandwidth guarantee for the VoIP traffic.
B. LLQ and CB-WRED should be implemented on the P router egress to support both VoIP and data traffic.
C. CBWFQ and CB-RTP header compression should be implemented on the P router egress to ensure minimum latency for VoIP traffic.
D. 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.

Answer: B

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:
1. RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
2. Using IP precedence or DSCP value of the packets, packets with higher precedence are less likely to be dropped. If the default settings are preventing QoS, the precedence value can be used to control how WRED determines when and how often to drop packets.
3. The amount of bandwidth used by the traffic flow. Flows that use the most bandwidth are more likely to have packets dropped.
4. The weight factor defined for the interface determines how frequently packets are dropped.
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 prioritybw
Router(config-pmap)#class class-default fair-queue
Router(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 342
Exhibit:

```
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 up tcp
```

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

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

Answer: D

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 343
What describes the use of best-effort service with over-provisioning?

A. ensuring quality of service by providing more than the aggregate bandwidth required
B. ensuring constant availability by provisioning multiple paths through the network
C. ensuring quality of service by deploying sophisticated prioritization and congestion management mechanisms
D. ensuring quality of service by being able to load balance across links in times of congestion
E. ensuring availability and quality of service by always provisioning key services across at least two service provider networks

Answer: A

Explanation:
Best-effort service with Overprovisioning means providing quality of service by providing more than the required bandwidth. So data packets doesn't drop due to the bandwidth problem.

QUESTION 344
The qos pre-classify command can be configured under which two configuration modes? (Choose two.)

A. router(config)#
B. router(config-if)#
C. router(config-pmap-c)#
D. router(config-crypto-map)#
E. router(config-cmap)#
F. router(config-router)#

Answer: B, D

Explanation:
This command is restricted to tunnel interfaces, virtual templates, and crypto maps. The qospre-classify command is unavailable on all other interface types.
Theqos pre-classify command can be enabled for IP packets only.
Examples
The following example enables the QoS for Virtual Private Networks (VPNs) feature on tunnel interfaces and virtual templates:
Router(config-if)# qos pre-classifyThe following example enables the QoS for VPNs feature on crypto maps:
Router(config-crypto-map)# qos pre-classify

QUESTION 345
Mission-critical traffic is not getting a minimum bandwidth of 192 kbps in this policy-map configuration:
policy-map test
class mission-critical
bandwidth 192
shape average 128000
queue-limit 64
What should be done to correct the problem?

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

Answer: C

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 346
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. 7 kbps
B. 10 kbps
C. 15 kbps
D. 28 kbps
E. 37 kbps
F. 56 kbps

Answer: F

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 347
Which three statements regarding WRED are true? (Choose three.)

A. WRED can be IP precedence-based or DSCP-based.
B. WRED is an advanced queuing mechanism.
C. ECN is an extension of WRED.
D. WRED is used to rate-limit the incoming traffic by metering the incoming traffic rate.
E. WRED can be applied to a traffic class using CB-WRED.
F. WRED uses a shaping queue to delay excess traffic.

Answer: A, C, E

Explanation:
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:
1. RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
2. Using IP precedence or DSCP value of the packets, packets with higher precedence are less likely to be dropped. If the default settings are preventing QoS, the precedence value can be used to control how WRED determines when and how often to drop packets.
3. The amount of bandwidth used by the traffic flow. Flows that use the most bandwidth are more likely to have packets dropped.
4. The weight factor defined for the interface determines how frequently packets are dropped.
WRED chooses the packets to drop after considering these factors in combination. The net result being that the highest priority and lowest bandwidth traffic is preserved.
WRED differs from standard random early detection (RED) in that RED ignores IP precedence, and instead drops packets from all traffic flows, not selecting low precedence or high bandwidth flows. By selectively dropping packets before congestion occurs, WRED prevents an interface from getting flooded, necessitating a large number of dropped packets. This increases the overall bandwidth usage for the interface

---

QUESTION 348
What are two errors in this policy-map configuration? (Choose two.)
policy-map test
class voice
priority 64
class bulk

bandwidth percent 20
fair-queue class interactive
bandwidth percent remaining 10
fair-queue class class-default fair-queue

A. The bandwidth command is missing for the class-default traffic class.
B. WFQ cannot be configured for the class-default traffic class.
C. WFQ cannot be configured for the bulk and interactive traffic classes.
D. The bandwidth units for the bulk and interactive traffic classes are inconsistent.
E. The priority command cannot be used with the bandwidth command within the same policy-map.
F. The voice traffic class should have the no fair-queue command.

Answer: C, D

Explanation:
Weighted Fair Queuing (WFQ) classifies traffic entering the queue based on traffic flows. The actual classification can be based on source and destination addresses, the protocol and TCP port numbers. Each flow is given its own queue. In its simplest form WFQ services each of these queues on a round robin basis. This means that every flow of traffic has an equal share of the available bandwidth, if it is required. Hence the term "fair" queue. The benefit for low volume traffic is reduced and predictable latency. For many applications this default behavior of WFQ is sufficient, however, some applications need specific QoS guarantees that require more than simply "fair" access to the bandwidth. In this case, the "weight" needs to be modified so that WFQ does not share bandwidth on a round-robin basis, but is influenced by the class or priority of the traffic in the flow.
Weighted fair queuing is activated on an interface using the fair-queue command:
Router(config)#interface serial 0/0
Router(config-if)#fair-queue

QUESTION 349
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 47
!
class-map match-any class 2
 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. The configuration is invalid since it refers to a class map within a different class.
B. The class-map class1 command will set the qos-group value to 4 for all IP packets.
C. Regardless of destination IP address, all traffic sent to Mac address 1.2.3 will be subject to policing
D. Only those packets which satisfy all of the matches in class1 and class2 will be subject to policing.
E. All traffic from a server with the IP address of 147.23.54.21 will be subject to policing.
F. Any IP packet will be subject to policing.

Answer: C, E

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 cisco
Switch(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:
1. Policy Name
2. Traffic class specified with the class command
3. QoS policies to be applied to each class
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 policy1
Switch(config-pmap)#class cisco
Switch(config-pmap-c)#bandwidth 3000
Switch(config-pmap-c)#exit
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#bandwidth 2000
Switch(config-pmap)#exit

QUESTION 350
Based on the following Cisco Catalyst 2950 Series switch configurations, which additional command will enable these actions? Traffic marked with a CoS of 6 or 7 will be serviced by the priority queue. Traffic marked with a CoS of 0, 1, or 2 will have a 20-percent weight when serviced by the wrr queue. Traffic marked with a CoS of 4 will have a 30-percent weight when serviced by the wrr queue. Traffic marked with a CoS of 3 or 5 will have a 50-percent weight when serviced by the wrr queue. Catalyst 2950 partial configuration: no wrr-queue cos-map wrr-queue cos-map 1 0 1 2 wrr-queue cos-map 2 4 wrr-queue cos-map 3 3 5 wrr-queue cos-map 4 6 7

A. wrr-queue bandwidth 1 10 15 25
B. wrr-queue bandwidth 1 20 30 50
C. wrr-queue bandwidth 15 25 10 1
D. wrr-queue bandwidth 10 15 25 0
E. wrr-queue bandwidth 15 25 10 0

Answer: D

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 351
Which two values influence how the fragment size should be set when configuring FRF.12? (Choose two.)

A. the physical interface port speed
B. the dual FIFO Frame Relay interface queue size
C. the CIR of the PVC
D. the Voice over IP (VoIP) packet size
E. the software queuing method

Answer: C, D

Explanation:
The purpose of end-to-end FRF.12 fragmentation is to support real-time and non-real-time data packets on lower-speed links without causing excessive delay to the real-time data. FRF.12 fragmentation is defined by the FRF.12 Implementation Agreement. This standard was developed to allow long data frames to be fragmented into smaller pieces (fragments) and interleaved with real-time frames. In this way, real-time and non-real-time data frames can be carried together on lower-speed links without

causing excessive delay to the real-time traffic.
End-to-end FRF.12 fragmentation is recommended for use on permanent virtual circuits (PVCs) that share links with other PVCs that are transporting voice and on PVCs transporting Voice over IP (VoIP). Although VoIP packets should not be fragmented, they can be interleaved with fragmented packets.
To configure the map class to support FRF.12 fragmentation, use the following map-class configuration command:

Command	Purpose
Router(config-map-class)# **frame-relay fragment** *fragment_size*	Configures Frame Relay fragmentation for the map class. The *fragment_size* argument defines the payload size of a fragment; it excludes the Frame Relay headers and any Frame Relay fragmentation header. The valid range is from 16 to 1600 bytes, and the default is 53. The value of *fragment_size* should be less than or equal to the MTU size. Set the fragmentation size such that the largest data packet is not larger than any voice packets.

QUESTION 352
Based on the Cisco Catalyst 2950 Series switch configuration shown, with no weights being assigned to the egress queues, which type of queuing is being implemented?
wrr-queue cos-map 1 0
wrr-queue cos-map 2 1 2 3
wrr-queue cos-map 3 4 5
wrr-queue cos-map 4 6 7

A. weighted round robin
B. priority
C. custom
D. weighted fair
E. weighted round robin with an expedite queue
F. modified deficit round robin

Answer: B

Explanation:
wrr-queue cos-map
To map CoS values to drop thresholds for a queue, use the wrr-queue cos-map command. Use the no form of this command to return to the default settings.
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
no wrr-queue cos-map

QUESTION 353
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. priority
B. bandwidth

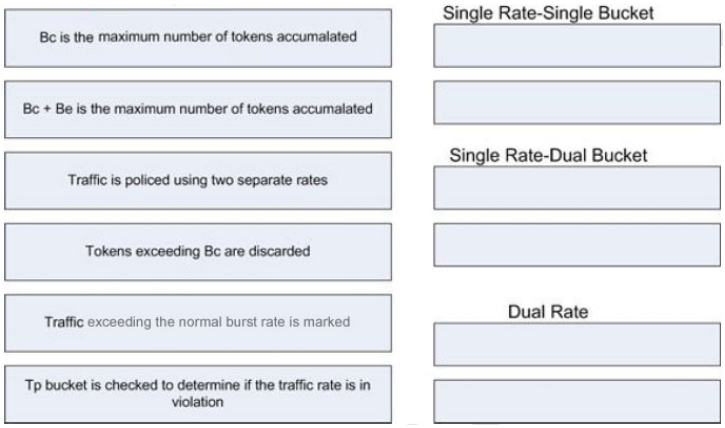
C. queue-limit
D. police
E. hold-queue

Answer: D

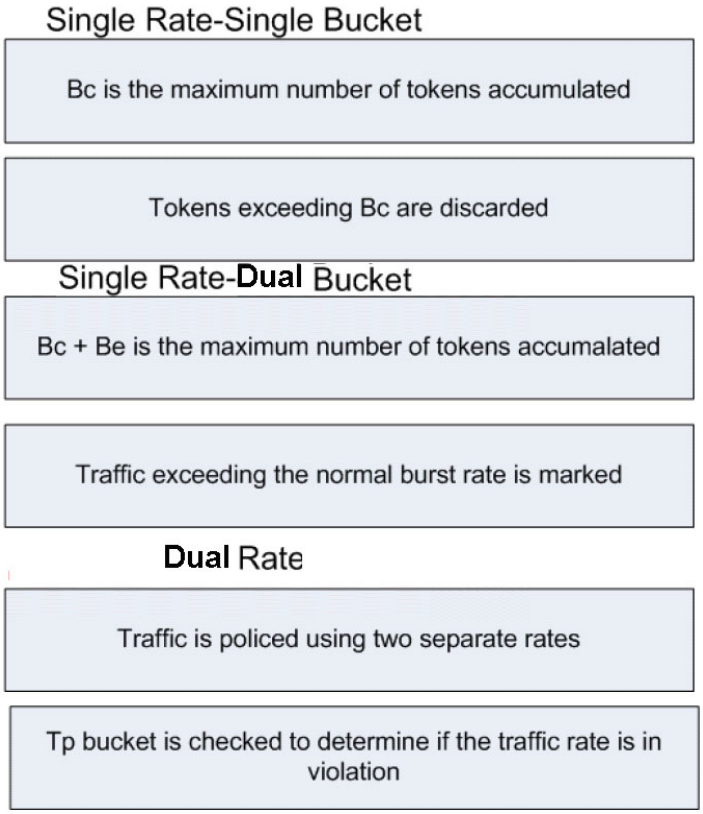
Explanation:
Individual policers apply the bandwidth limits specified in the policer separately to each matched traffic class. This type of policer is configured within a policy map using the police policy-map configuration command.
The format of the police command on the Catalyst 3550 is as follows:
police rate-bps burst-byte [exceed-action {drop|policed-dscp-transmit}]
The police on an IOS-based router operates in a similar fashion except that the actual DSCP values are specified as part of the command line rather than being specified as a separate translation table, as is the case on a Catalyst Switch. IOS-based routers also permit IP Precedence to be set

---

QUESTION 354
DRAG DROP
Put each statement on the left to the proper traffic policing method on the right
Exhibit:



Answer:

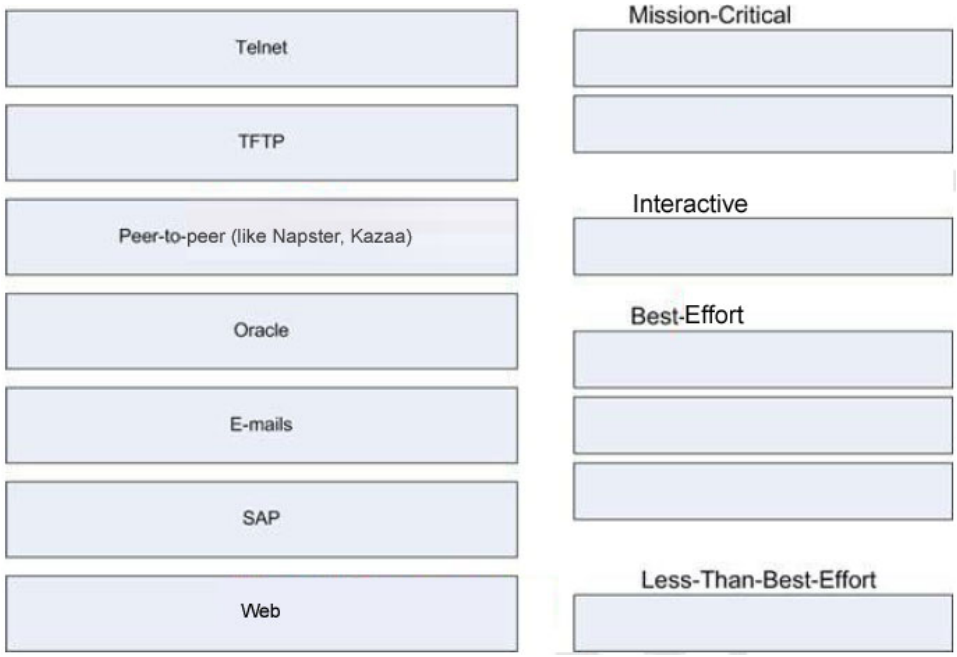


QUESTION 355

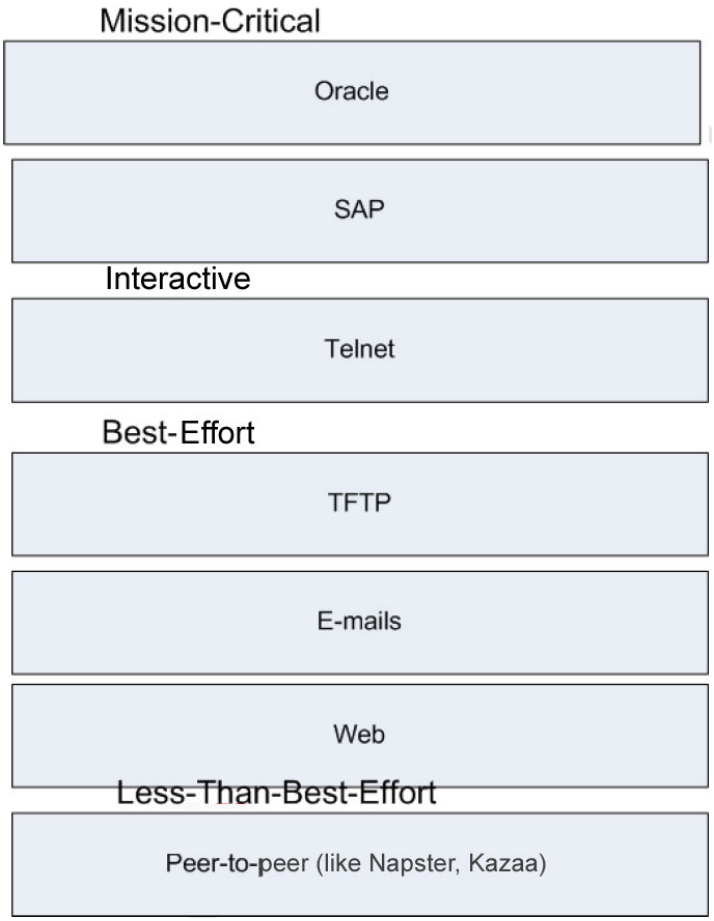
DRAG DROP

Put the application type on the left to the most appropriate traffic class on the right.

Exhibit



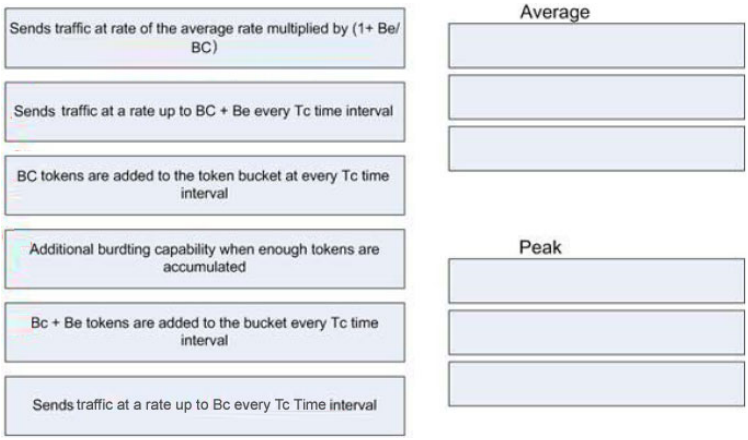
Answer:



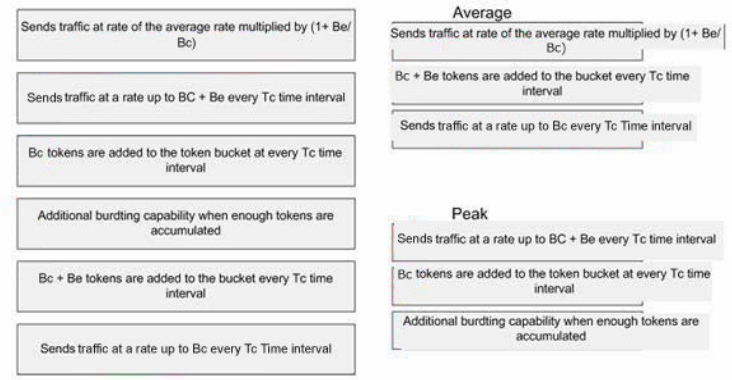
Explanation:
Increasingly data networks are being called upon to support communications for traffic with varied delivery requirements. Previously an organization used separate networks for voice, video, and data traffic. It is now common practice to combine these into a single multiservice network in which the varied traffic types coexist. There are many circumstances where these Quality of Service (QoS) requirements have not been met or even addressed at a rudimentary level:
1. The long delay in speech transmission when calling by way of an international satellite link
2. Stop-start and choppy Internet streaming video performance
3. Harsh audio when using an Internet-based IP phone
4. Messenger applications are all examples of inadequate QoS
For many applications such as file and print services, Internet browsing, email and peer-to-peer messaging products, the "best effort" delivery attempts of the Internet and many corporate networks may be adequate. However, for organizations seeking to integrate their voice and data networks using Voice over IP (VoIP), IP telephony or high quality streaming video for corporate communications, it is essential that QoS be built into the design of the network.
In order to provide QoS within a network it is critical to have an understanding of the network characteristics that make up quality of service and the QoS requirements of the varied traffic and applications using the network. Once application and traffic

requirements can be stated in QoS terms, classification techniques are used to identify streams of traffic as having a particular QoS requirement. For example, a standard access-list could be used to identify a user who requires priority access to the network resources. Once traffic has been classified into classes of service, there are many scheduling and congestion management techniques that can be used to provide the desired service characteristics. The key to effective QoS design is knowing how these techniques operate and the benefits and limitations of each.

QUESTION 356
DRAG DROP
Put each statement on the left beneath the appropriate traffic shaping method on the right.
Exhibit:



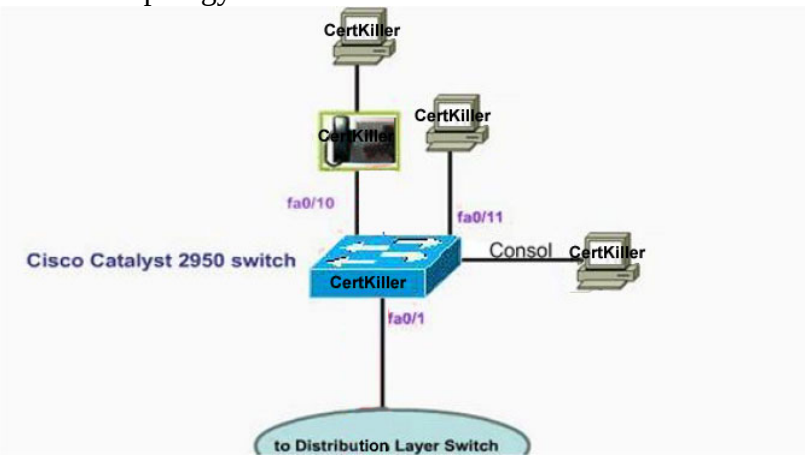
Answer:



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.
Traffic shaping prevents packet loss. Its use is important in Frame Relay networks because a Frame Relay switch cannot determine which packets take precedence, and which packets should be dropped when congestion occurs. It is of critical importance for real-time traffic, such as Voice over Frame Relay, that latency be minimized by bounding

the amount of traffic and traffic loss in the data link network and by keeping the data in the router that is making the guarantees.
Retaining the data in the router, through the use of queuing, allows the router to prioritize traffic according to the guarantees it is making.
Cisco IOS QoS software has three types of traffic shaping:
1. Generic Traffic Shaping (GTS)
2. Class-Based
3. Frame Relay Traffic Shaping (FRTS)
All three of these traffic shaping methods are similar in implementation, though the CLIs differ somewhat and they use different types of queues to contain and shape traffic that is deferred. The underlying code that determines whether enough credit is in the token bucket for a packet to be sent or whether that packet must be delayed is common to both features. If a packet is deferred, GTS and Class-Based Shaping use a weighted fair queue to hold the delayed traffic. FRTS uses either a custom queue or a priority queue for the same, depending on what has been configured.

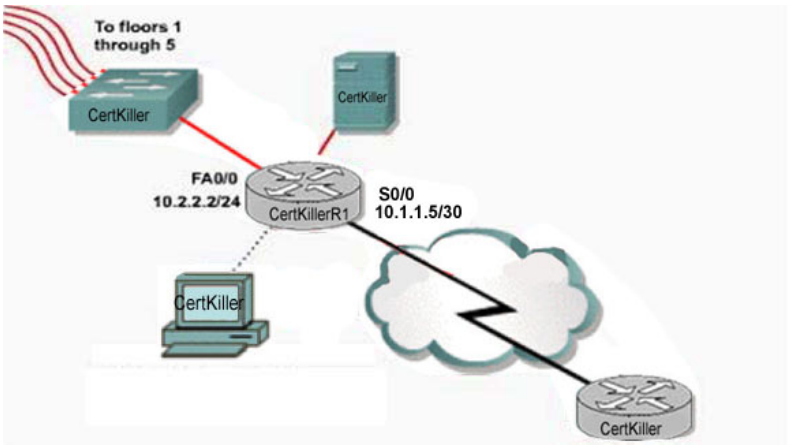
QUESTION 357
You work as a Certkiller .com network administrator in Johannesburg South Africa.
Network topology exhibit:



For scenario we refer to the iPAD document.
Configure the fa0/0 and fa0/11 ports on the Cisco Catalyst 2950 switch as follows:
On port fa0/1, trust all incoming DSCP settings.
On port fa0/11, trust all incoming CoS settings.
On port fa0/10, trust the incoming CoS setting only if a Cisco IP Phone is connected to the fa0/10 port: otherwise do not trust any CoS or DSCP markings coming in.
** Incomplete ***

Answer:

QUESTION 358
Exhibit:



You work as a network technician at Certkiller .com office in Tokyo.
On the Certkiller R1 WAN edge router, configure the appropriate MQC based queuing mechanism for the outbound traffic to the WAN (S0/0) so that the following bandwidth requirements will be met. A strict priority queue with a 168 Kbps bandwidth guarantee for the class voice is reserved, a minimum bandwidth guarantee of 30 Kbps is configured for the class interactive, a minimum bandwidth guarantee of 16 Kbps for class bulk, and the default class is configured for WFQ with no bandwidth guarantee.
In addition, also limit the bulk traffic class to an average rate of 24 Kbps by buffering excess traffic(use the IOS default Bc and Be)
** Incomplete ***

Answer:

QUESTION 359
Which two of the following are considered QoA best practices, considering a typical converged campus network? (Choose two.)

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

Answer: