Cisco 642-642

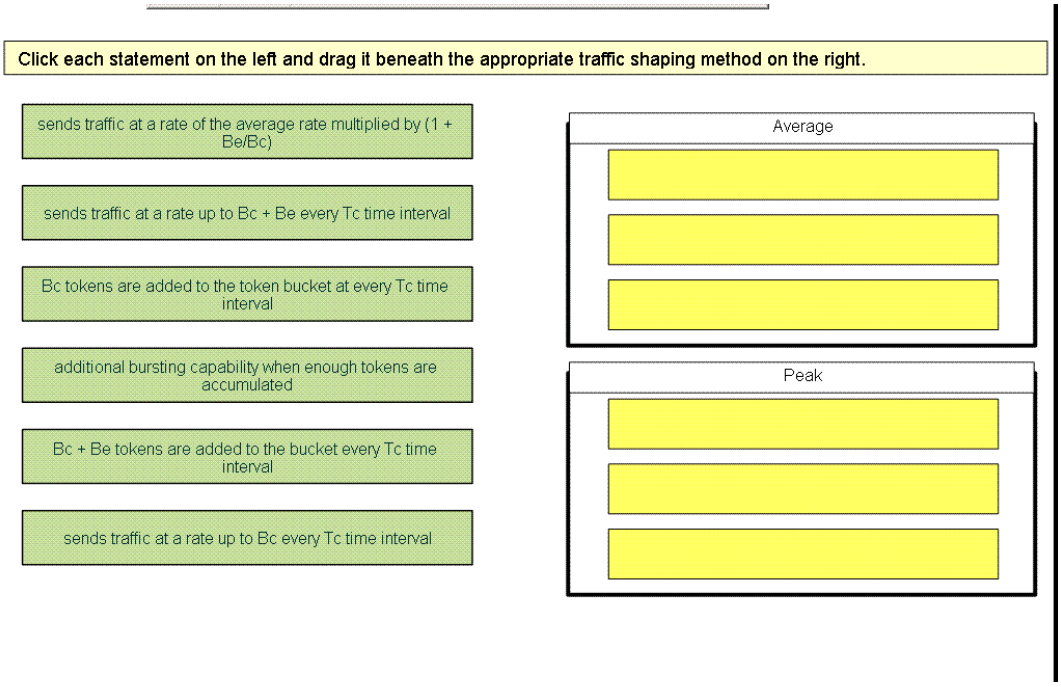
Quality of Service (QoS)

Version: 4.2

Topic 1, Volume A

QUESTION NO: 1 DRAG DROP

Drop



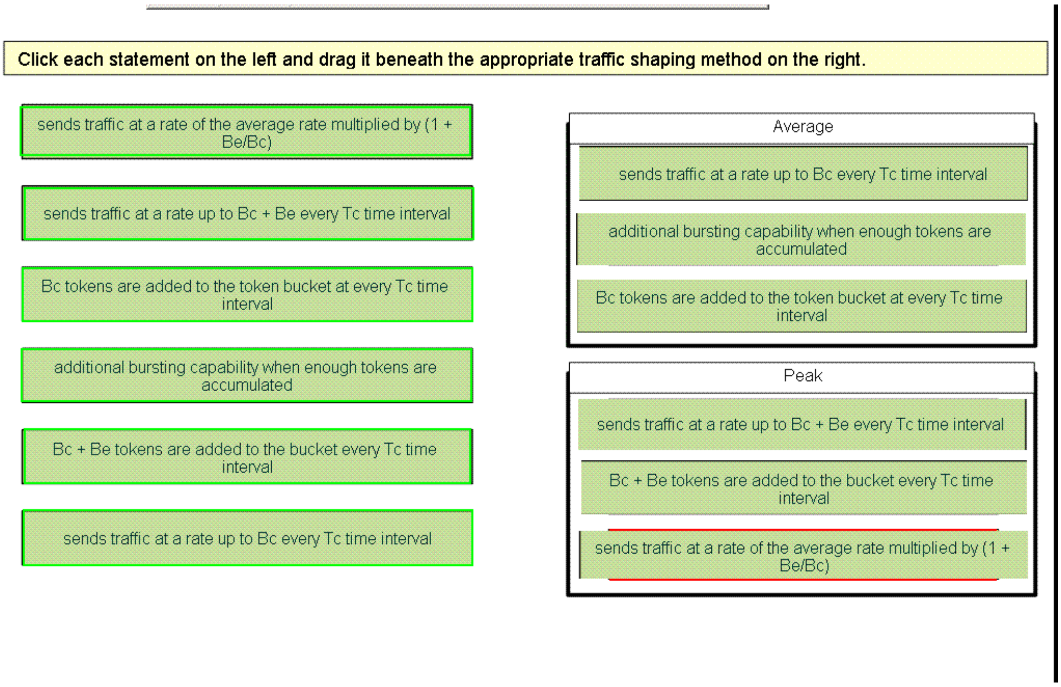
Click each statement on the left and drag it beneath the appropriate traffic shaping method on the right.

- sends traffic at a rate of the average rate multiplied by (1 + Be/Bc)
- sends traffic at a rate up to Bc + Be every Tc time interval
- Bc tokens are added to the token bucket at every Tc time interval
- additional bursting capability when enough tokens are accumulated
- Bc + Be tokens are added to the bucket every Tc time interval
- sends traffic at a rate up to Bc every Tc time interval

Average

Peak

Answer:



Click each statement on the left and drag it beneath the appropriate traffic shaping method on the right.

- sends traffic at a rate of the average rate multiplied by (1 + Be/Bc)
- sends traffic at a rate up to Bc + Be every Tc time interval
- Bc tokens are added to the token bucket at every Tc time interval
- additional bursting capability when enough tokens are accumulated
- Bc + Be tokens are added to the bucket every Tc time interval
- sends traffic at a rate up to Bc every Tc time interval

Average

- sends traffic at a rate up to Bc every Tc time interval
- additional bursting capability when enough tokens are accumulated
- Bc tokens are added to the token bucket at every Tc time interval

Peak

- sends traffic at a rate up to Bc + Be every Tc time interval
- Bc + Be tokens are added to the bucket every Tc time interval
- sends traffic at a rate of the average rate multiplied by (1 + Be/Bc)

Explanation:

QUESTION NO: 2

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

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

Answer: D
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 NO: 3

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

A. LLQ, CB-WRED, CB-Marking, FRTS, FRF.12, and CB-RTP header compression
B. CBWFQ, FRTS, FRF.12, and CB-RTP header compression
C. WRR, CB-WRED, CB-Marking, FRF.12, and CB-RTP header compression

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

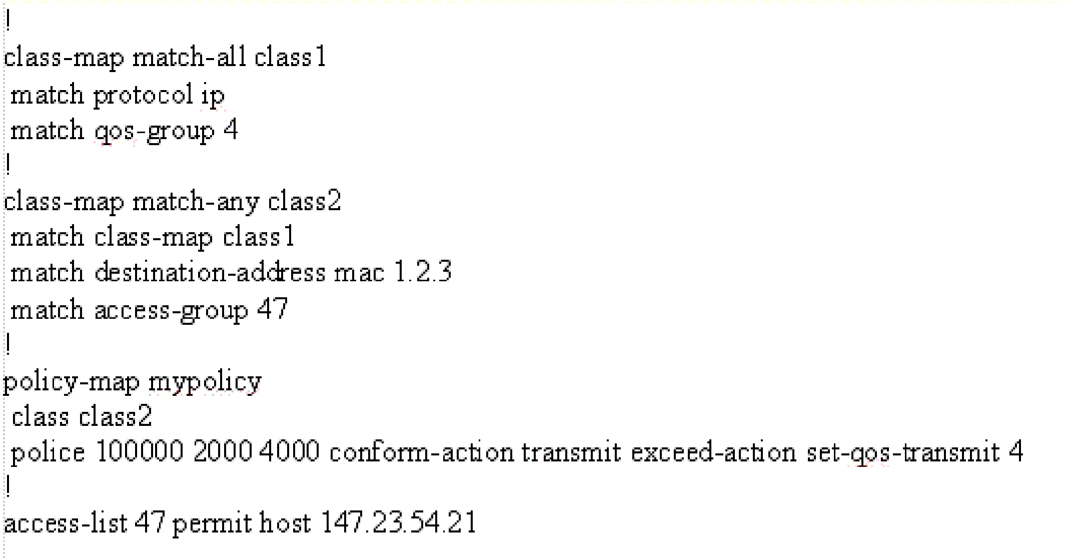
Answer: A
Explanation:

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 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 NO: 4

Refer to the partial router configuration. Which two of the following statements are true? (Choose two.)



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

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

Answer: A,B
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:

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 NO: 5

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

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

Answer: C
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 NO: 6

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

A. mls qos trust device cisco-phone

B. switchport priority extend trust
C. mls qos trust cos
D. no mls qos trust dscp
E. mls qos trust extend [cos value]
F. mls qos cos 5

Answer: A,C
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 NO: 7

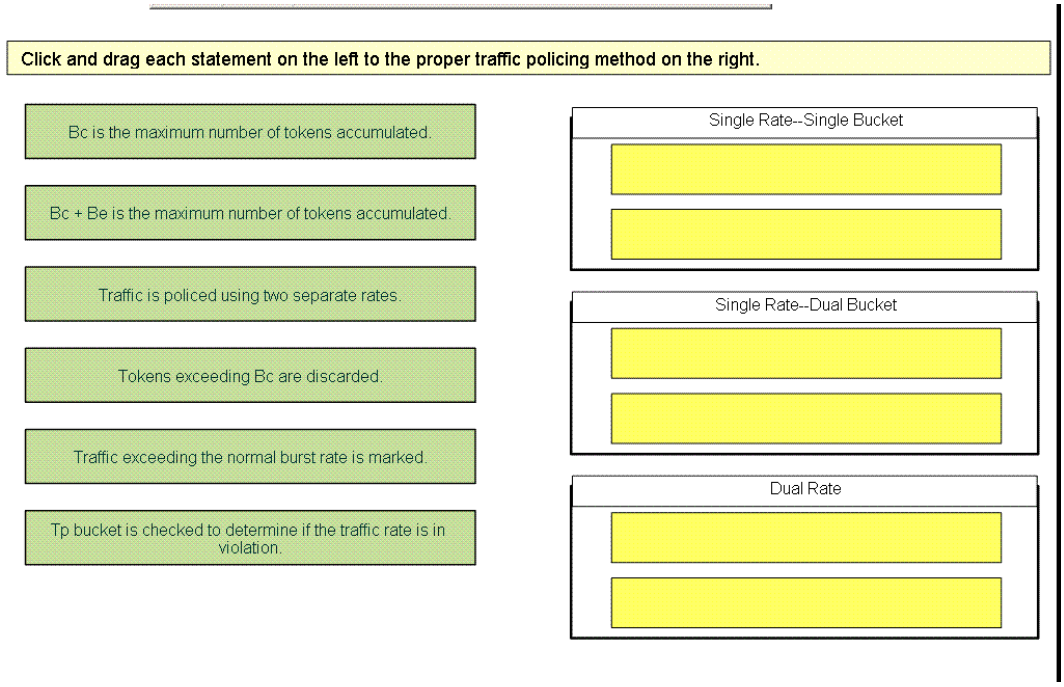
According to the best practices, in a service provider network, which statement is true as related to the QoS policy that should be implemented on the inbound provider (P) to provider (P) router link?

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

Answer: D
Explanation:

QUESTION NO: 8 DRAG DROP

Drop



Click and drag each statement on the left to the proper traffic policing method on the right.

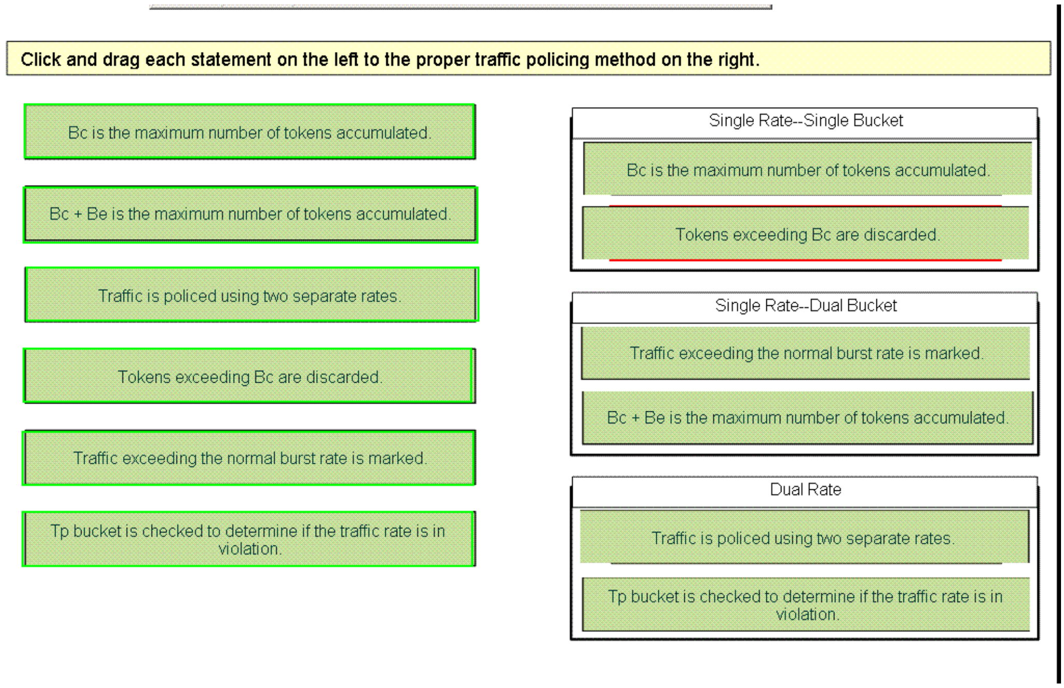
- Bc is the maximum number of tokens accumulated.
- Bc + Be is the maximum number of tokens accumulated.
- Traffic is policed using two separate rates.
- Tokens exceeding Bc are discarded.
- Traffic exceeding the normal burst rate is marked.
- Tp bucket is checked to determine if the traffic rate is in violation.

Single Rate--Single Bucket

Single Rate--Dual Bucket

Dual Rate

Answer:



Click and drag each statement on the left to the proper traffic policing method on the right.

- Bc is the maximum number of tokens accumulated.
- Bc + Be is the maximum number of tokens accumulated.
- Traffic is policed using two separate rates.
- Tokens exceeding Bc are discarded.
- Traffic exceeding the normal burst rate is marked.
- Tp bucket is checked to determine if the traffic rate is in violation.

Single Rate--Single Bucket
- Bc is the maximum number of tokens accumulated.
- Tokens exceeding Bc are discarded.

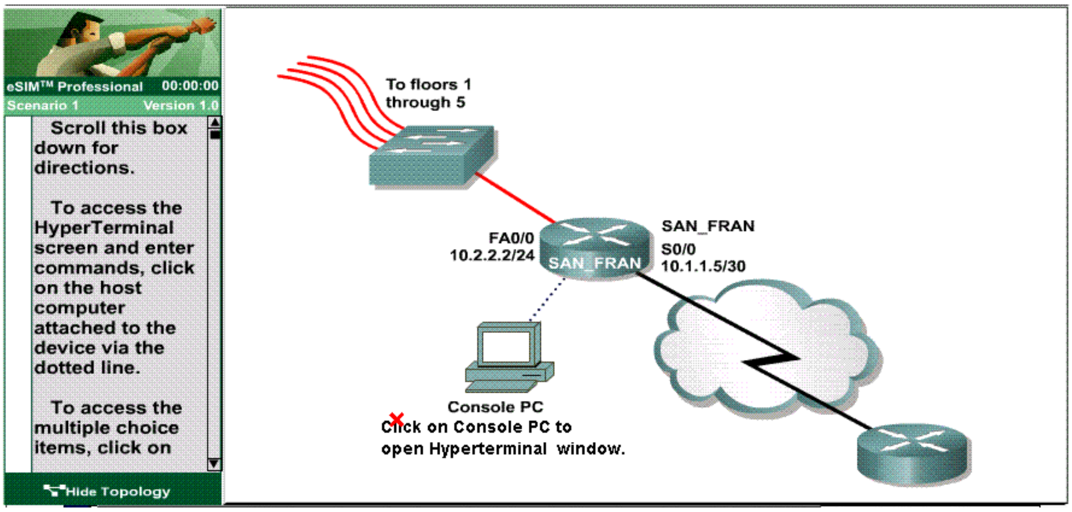
Single Rate--Dual Bucket
- Traffic exceeding the normal burst rate is marked.
- Bc + Be is the maximum number of tokens accumulated.

Dual Rate
- Traffic is policed using two separate rates.
- Tp bucket is checked to determine if the traffic rate is in violation.

Explanation:

QUESTION NO: 9 HOTSPOT

HOTSPOT

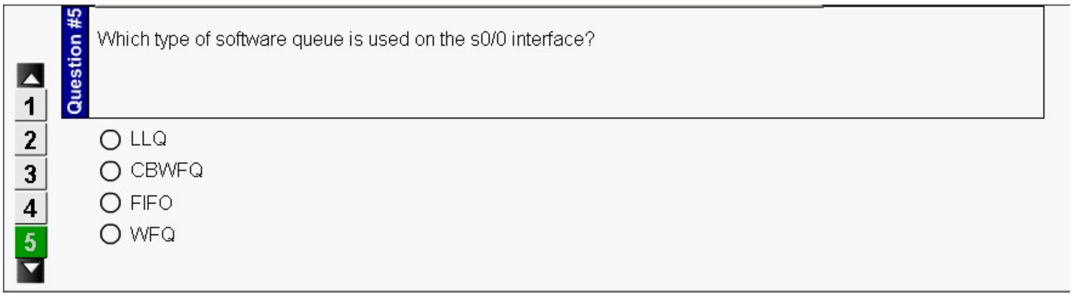


Scroll this box down for directions.

To access the HyperTerminal screen and enter commands, click on the host computer attached to the device via the dotted line.

To access the multiple choice items, click on

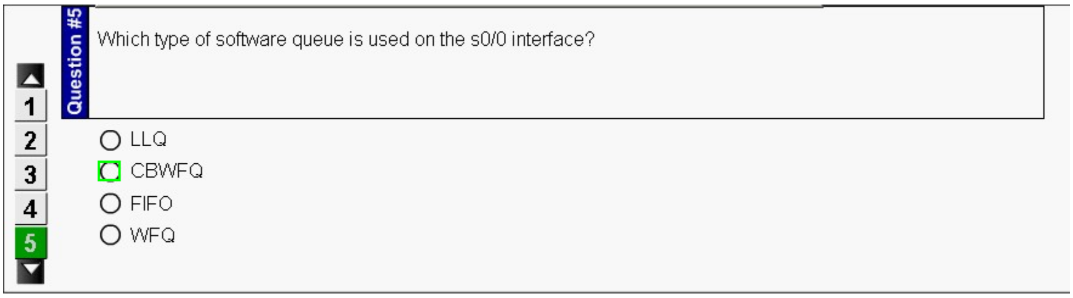
Click on Console PC to open Hyperterminal window.



Which type of software queue is used on the s0/0 interface?

○ LLQ
○ CBWFQ
○ FIFO
○ WFQ

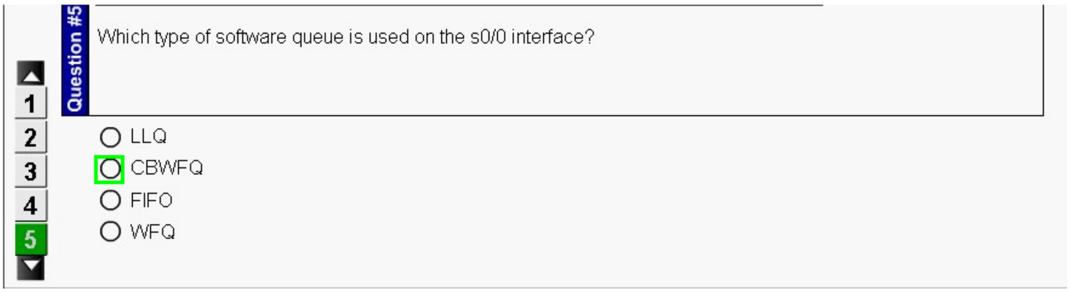
Answer:



Which type of software queue is used on the s0/0 interface?

○ LLQ
[✓ CBWFQ]
○ FIFO
○ WFQ

Explanation:



Which type of software queue is used on the s0/0 interface?

○ LLQ
[✓ CBWFQ]
○ FIFO
○ WFQ

QUESTION NO: 10

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

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

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

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 NO: 11

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

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

FastEthernet0/1

trust state: not trusted
```