Chapters 13 – 14: Multicast and QoS Exam (Answers)

itexamanswers.net/chapters-13-14-multicast-and-qos-exam-answers.html

CCNPv8 ENCOR (Version 8.0) – Multicast and QoS Exam

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. What is the IP address for the Cisco-RP-announce multicast group?
- 224.0.1.49
- 224.0.0.1
- 224.0.0.40
- **224.0.1.39**

Explanation: The internet Assigned Numbers authority has assigned two group addresses, 224.0.0.39 and 224.0.1.40, for Auto-RP configuration in order to announce the RP in the multicast group.

2. Which is a characteristic of PIM sparse mode?

- It uses a pruning mechanism to stop the flow of unwanted multicast traffic on interfaces with no downstream neighbors.
- **It requires an RP on the network to act as the root of the shared distribution tree.**
- It builds the multicast tree by flooding traffic out all interfaces.
- It is designed for networks where receivers are located on every subnet in the network.

Explanation: PIM sparse mode chooses one or more routers to operate as rendezvous points (RPs). An RP is a single common root placed at a chosen point of a shared distribution tree.

3. The bootstrap router (BSR) mechanism of automating the distribution of rendezvous point (RP) information uses which IP address to disseminate information to all protocol independent multicast (PIM) routers?

- 224.1.0.13
- **224.0.0.13**
- 224.1.1.13
- 224.0.1.13

Explanation: BSR (bootstrap router) messages are forwarded out of every PIM-enabled interface and use the all PIM router address 224.0.0.13 with a TTL of 1.

4. A network administrator is troubleshooting an IP multicast problem. Where can the administrator view source S, group G, incoming interfaces (IIF), outgoing interfaces (OIFs), and RPF neighbor information for each multicast route?

- in unicast routing table
- in the routing information base
- in the multicast forwarding information base
- **in the multicast routing information base**

Explanation: The multicast routing information base (MRIB) is a topology table that is also known as the multicast route table (mroute). The MRIB is built using PIM and the routing table. It contains the source S, group G, incoming interfaces (IIF), outgoing interfaces (OIFs), and RPF neighbor information for each multicast route as well as other multicast-related information. The command show ip mroute is used to display the full contents of the IP multicast routing table.

5. A network administrator statically assigns a multicast address of 239.255.8.5 to an application running on a server. The NIC on the server is with the MAC address of AB.54.C1.01.B8.9F. Which Layer 2 multicast address will receivers use on their interfaces in order to receive the multicast feed?

- 01:00:5E:01:B8:9F
- AB:54:C1:17:A8:02
- **01:00:5E:7F:08:05**
- AB:54:C1:7F:08:05

Explanation: When a receiver wants to receive multicast feed from a particular multicast service, it will send a IGMP join message with the multicast IP address of the service and then reprogram the receiver interface with the matching multicast MAC address. To find the matching MAC address, do the following:

Convert the IP multicast address 239.255.8.5 to binary form,
11101111.11111111.00001000.00000101
Separate the 23 low-order binary bits from the converted address,
1111111.00001000.00000101

Convert these bits to hexadecimal: 7F:08:05
Because the first 24bits of a multicast MAC address are 01.00.5E, The resulting multicast MAC address is then 01:00:5E:7F:08:05.

6. Which notation is used to refer to the forwarding state in PIM shared trees?

- **(*,G)**
- (S,G)
- (*,S)
- (G,S)

Explanation: In a shared tree uses a rendezvous point (RP) as the tree root instead of the multicast source. Multicast traffic is forwarded down the shared tree to the group address (G). For this reason the forwarding state is referred to as (*,G).

7. Which statement about IGMPv3 is true?

- It sends IGMP query messages with a TTL value of 1 addressed to the all-host group (224.0.0.1).
- It rejects any group-specific query message that is sent from the hosts that want to join a multicast group.
- **It enables a multicast receiver to signal to the first hop router the multicast sources from which it expects to receive traffic.**
- It does not accept a leave group message from the hosts that have already joined the multicast group.

Explanation: IGMPv3 is an extension of IGMPv2 with added support for multicast source filtering done through the use of a new message type called Version 3 membership report. It supports applications that explicitly signal sources that want to receive multicast traffic by using the membership report in the Include or Exclude mode.

8. Which well-know multicast group is joined by all PIM-enabled routers to receive RP mappings?

- 224.0.0.2
- 224.0.0.13
- **224.0.1.40**
- 224.0.1.39

Explanation: RP mapping agents advertise the RP mappings to the well-known multicast group address, 224.0.1.40 (Cisco-RP-Discovery). Advertisements are sent every 60 seconds by default, or when changes are detected. All PIM-enabled routers join 224.0.1.40 and store the RP mappings in cache.

9. An administrator has configured and enabled multicast together with PIM sparse mode on all VLANs on the network. Which feature helps to reduce multicast traffic being broadcast on the access layer switches?

- source registration
- PIM Pruning
- **IGMP snooping**
- SPT switchover

Explanation: IGMP snooping stops multicast traffic from being broadcast on the access layer switches by examining IGMP joins that are sent by receivers and maintaining a table of interfaces to IGMP joins.

10. Which two IGMPv3 modes are used to signal membership to a multicast host group? (Choose two.)

- preclude
- join
- **include**
- rendezvous
- **exclude**
- leave

Explanation: The two IGMP modes that are used to signal membership are Include mode (the receiver announces membership to a multicast group and provides a include list) and Exclude mode (receiver announces membership to multicast group and provides exclude list).

11. Which statement describes a characteristic of IP multicast routing?

- PIM hello messages are sent every 60 seconds by default out each PIM enabled interface.
- **PIM dense mode flood and prune behavior repeats every three minutes.**
- PIM sparse mode builds the multicast tree through flooding of traffic out every interface.
- PIM sparse mode and PIM dense mode require an RP on the network.

Explanation: PIM dense mode is used in a multicast group that is densely populated across the network. PIM dense mode (PIM-DM) prunes expire after three minutes. This means that the flood and prune behavior of PIM dense mode repeats every three minutes and should be taken into account when designing a network for PIM-DM. A rendezvous point (RP) is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM).

12. To which multicast group does a candidate RP send announcement messages to advertise its willingness to be an RP?

- 224.0.0.13
- 224.0.1.40
- **224.0.1.39**
- 224.0.0.2

Explanation: A C-RP advertises its willingness to be an RP every 60 seconds via RP announcement messages to the reserved well-known multicast group 224.0.1.39 (Cisco-RP-Announce). RP mapping agents join group 224.0.1.39 to receive the RP announcements.

13. Which two statements about Protocol Independent Multicast (PIM) are true? (Choose two.)

- **Three of the forwarding modes for PIM are PIM dense mode (PIM-DM), PIM sparse mode (PIM-SM), and PIM sparse-dense mode.**
- **PIM is a multicast routing protocol that makes packet-forwarding decisions independent of the unicast IP routing protocol that is running in the network.**
- PIM should be configured on the device that hosts the source of the muticast traffic.
- PIM sparse mode is most useful when there are few senders, many receivers, and the volume of multicast traffic is high.
- PIM should be configured only on the first and the last hop routers in the multicast tree.
- PIM does not require an IGP protocol to be configured in the network.

Explanation: PIM is a multicast routing protocol that routes multicast traffic between network segments by creating distribution trees. It makes packet-forwarding decisions independent of the unicast IP routing protocol that is running in the network. There are five operating PIM modes:

PIM dense mode (PIM-DM)

PIM sparse mode (PIM-SM)

PIM sparse dense Mode

PIM source specific multicast (PIM-SSM)

PIM bidirectional mode (Bidir-PIM)

14. Which two statements describe IGMP? (Choose two.)

- IGMPv2 supports multicast source filtering.

- IGMPv1 only supports queries sent to a predefined group.
- **IGMPv3 provides support for SSM.**
- An IGMPv2 router will only allow IGMPv2 hosts to execute a join request.
- **Multicast flooding on a LAN segment can be mitigated by using IGMP snooping.**

Explanation: IGMPv3 is used to provide source filtering for Source Specific Multicast (SSM). IGMP snooping can be used to mitigate multicast flooding and optimize the forwarding of multicast traffic to interested receivers.

15. Which nonproprietary mechanism does PIM use to discover and announce RP set information for each group prefix for all the routers in a PIM domain?
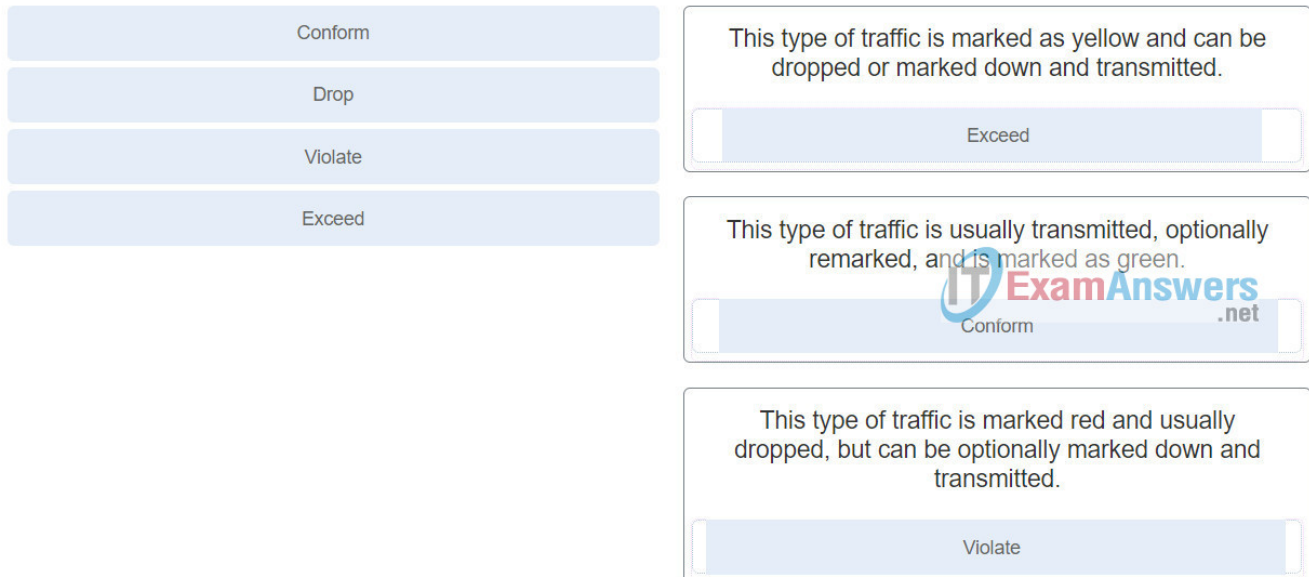
- Static RP
- **BSR**
- RPF
- Auto-RP

Explanation: The bootstrap router (BSR) mechanism is used by PIM to discover and announce RP set information for each group prefix for all the routers in a PIM domain. This mechanism provides a fault-tolerant, automated RP discovery and distribution mechanism.

16. What happens when an edge router using IntServ QoS determines that the data pathway cannot support the level of QoS requested?

- Data is forwarded along the pathway using IntServ but not provided preferential treatment.
- Data is forwarded along the pathway using DiffServ.
- Data is forwarded along the pathway using a best-effort approach.
- **Data is not forwarded along the pathway.**

Explanation: When the IntServ QoS model is being used, if network devices along a data path can reserve the required bandwidth, the originating application can begin transmitting. If the requested resource reservation cannot be allocated along the path, the originating application does not send any data.

17. Question as presented: Match the state with its marking in a DSCP two token bucket mechanism environment. (Not all options apply.)

Conform	This type of traffic is marked as yellow and can be dropped or marked down and transmitted.
Drop	Exceed
Violate	This type of traffic is usually transmitted, optionally remarked, and is marked as green.
Exceed	Conform
	This type of traffic is marked red and usually dropped, but can be optionally marked down and transmitted.
	Violate

18. What two fields are available in IPv4 and IPv6 headers to mark packets for QoS? (Choose two.)

- **Traffic Class**
- Class of Service
- **Type of Service**
- Priority
- VLAN ID

Explanation: IPv4 uses an 8-bit Type of Service field to mark packets at Layer 3 and IPv6 uses an 8-bit Traffic Class field to mark packets at Layer 3. The fields are used by receiving devices to forward the packets based on the appropriate assigned QoS policy.

19. A network administrator has defined the trust boundary of a network. What is the function of trusted endpoints deployed across the network?

- Trusted endpoints are devices designed to provide network security features.
- Trusted endpoints provide monitoring and logging solutions.
- **Trusted endpoints have the ability to mark application traffic.**
- Trusted endpoints provide the ability to drop previously marked traffic during congestions.

Explanation: Trusted endpoints are devices that have the capability to mark application traffic at Layer 2 or Layer 3. Trusted endpoints include the following:
IP phones
Wireless access points
Videoconferencing gateways and systems
IP conferencing stations and more

20. Which is a QoS model that a network engineer would implement to ensure a source to destination quality of service standard for a specified data flow?

- best effort
- low latency queuing
- differentiated services
- class-based weighted fair queuing
- **integrated services**

Explanation: Best effort is the default packet forwarding design and provides no QoS. The differentiated services model enforces and applies QoS mechanisms on a hop-by-hop basis, not source to destination. Class-based weighted fair queuing and low latency queuing are queuing algorithms.

21. What would be the Tc value in ms for a 1 Gbps interface configured with a policer defined with a CIR of 150 Mbps and a Bc of 12 Mb?

- 10,000 ms
- 1000 ms
- **100 ms**
- 10 ms

Explanation: The Tc value is calculated by using the formula Bc (bits)/ CIR (bps) X 1000
TC = (15 Mb/150 Mbps) X 1000
Tc = (15,000,000 bits/150,000,000 pbs) X 1000
Tc = 100 ms

22. What statement describes the Class of Service field?

- **It is a Layer 2 field.**
- It is a field that is 6 bits long.
- It is a field that is 8 bits long.
- It is a Layer 1 field.

Explanation: The Class of Service is a 3-bit, Layer 2 field that is used as part of quality of service (QOS) between switches. The CoS is also one of the values used for classification and marking of traffic.

23. Which protocol operates at Layer 3 and is used for marking packets?

- CoS
- IntServ
- **DSCP**
- QoE

Explanation: The differentiated services code point (DSCP) protocol is used to mark a 6-bit field within the DiffServ field that allows for classification of up to 64 values used for QoS.

24. What is the recommended maximum one-way latency when implementing video over IP for real-time video applications?

- Latency is not a factor for smooth video over IP implementation.
- Latency should be defined for voice traffic only (not for video).
- **The recommended maximum one-way latency should not be more than 150 ms.**
- When mixed video and voice packets are included in the video stream, the latency should be 300 ms.

Explanation: Because voice traffic is very sensitive to delay and jitter, to avoid packet drops care must taken to be ensure a maximum one-way latency of not more then 150ms.

25. Which two procedures should be implemented when deploying VoIP in a campus network? (Choose two.)

- voice and data traffic in the same VLAN and mark the traffic for high priority treatment
- a traffic shaping QoS policy to guarantee minimum delay for the voice traffic
- **packet marking for voice traffic with a 802.1p CoS value of 5**
- priority queuing with voice traffic given the high-priority queue
- **a voice class low-latency queuing (LLQ) QoS policy**

Explanation: Because voice traffic is very sensitive to latency and jitter, it would be better to keep it on a separate vlan and prioritize the traffic using QoS mechanisms. Such actions will ensure that the voice traffic has a dedicated bandwidth that is sufficient to meet its needs and the traffic is marked as priority over any other traffic.

26. Which statement is true about the Single-Rate Two-Color Markers algorithm?

- It uses a two bucket algorithm and traffic can be classified as conforming to, exceeding, or violating the CIR.
- **It uses a single token bucket algorithm and traffic can be marked or dropped in both states (conforming to or exceeding the CIR).**
- It uses a two bucket algorithm that causes fewer TCP transmissions and is more efficient for bandwidth utilization.
- It uses a single bucket algorithm and uses three colors or states to classify the traffic.

Explanation: The Single-Rate Two-Color Markers use a single token algorithm while the Single-Rate Three-Color markers use the two token bucket algorithm.

27. Question as presented: Match the queuing algorithm with its description. (Not all options apply.)

WFQ
Round Robin
CBWFQ
LLQ
PQ
CQ

This enables the creation of 256 queues, serving up to 256 traffic classes. Each queue is based on the bandwidth assigned to that class.

CBWFQ

This can serve up to 256 classes of traffic and is combined with priority queueing to meet the requirements of real time traffic.

LLQ

This algorithm automatically divides the interface bandwidth by the number of flows (weighted by IP precedence) to allocate bandwidth fairly among all flows.

WFQ

This algorithm uses a set of 4 queues (high, medium, normal and low) and are served in strict priority order.

PQ

This algorithm services all queues in sequence with only one packet being serviced in each queue at any given time.

Round Robin

28. What is the value of the DSCP marker for video traffic on a WLAN?

- **AF41**
- O
- AF11
- EF

Explanation: The traffic types and their associated DSCP values in a WLAN are as follows:
Voice-EF
Video-AF41
Best Effort-O
Background-AF11

29. Which statement describes NBAR2?

- NBAR2 can identify a variety of protocols and applications by using up to Layer 6 data.
- NBAR2 supports only scavenger traffic.
- **NBAR2 uses MQC to match traffic to specific protocols.**
- NBAR2 does not require monthly protocol packs to identify new and emerging applications.

Explanation: NBAR2 is a deep packet inspection engine that uses Layer 3 through 7 data to identify a variety of protocols. it can operate in either Protocol discovery mode or Modular QoS CLI (MQC) mode.

30. Match QoS techniques with the description. (Not all options are used.)

| traffic policing |
| marking |
| traffic shaping |
| classification |

Excess traffic is retained in a queue and scheduled for later transmission over increments of time.

traffic shaping

Excess traffic is dropped when the traffic rate reaches a preconfigured maximum.

traffic policing

This determines the class of traffic to which frames belong.

classification

A value is added to a packet header.

marking

TCP traffic is throttled to prevent tail drop.

31. Match the parameter with the correct description. (Not all options apply.)

CIR

Tc

Bc

CoS

allows for grouping of similar types of traffic for traffic shaping and policing
CoS

the time interval over which the committed burst of traffic is sent
Tc

the policed traffic rate as defined in the traffic contract
CIR

32. Match the operation to the appropriate QoS model.

Network devices are setup to handle multiple traffic classes.

End-to-end QoS is provided.

Traffic is identied in classes based on business requirements.

QoS is not enabled for this model.

Network resources are requested.

No packets receive preferential treatment.

Best Effort

QoS is not enabled for this model.

No packets receive preferential treatment.

IntServ

End-to-end QoS is provided.

Network resources are requested.

DiffServ

Network devices are setup to handle multiple traffic classes.

Traffic is identied in classes based on business requirements.