Chapter 13: Quiz – Multicast (Answers) CCNPv8 ENCOR

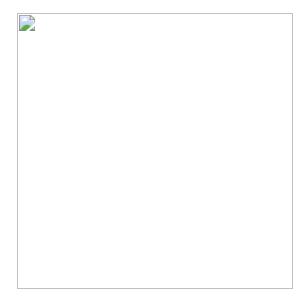**itexamanswers.net**/chapter-13-quiz-multicast-answers-ccnpv8-encor.html

January 11, 2021

16. Refer to the exhibit. When considering the route map configuration for BGP, what is the result when inbound traffic is received with a source IP that matches ACL1?

- The incoming network traffic will go through the whole route map.
- **The optional action is processed, and the route map completes.**
- If the incoming network traffic does not match ACL2 and ACL3, it will be dropped.
- The optional action is processed, and route map continues to test with ACL2.

Explanation: A route map uses the command syntax **route-map** *route-map-name* [**permit** | **deny**][*sequence-number*]. The rules that apply to route map statements are as follows:

- If a processing action is not provided, the default value **permit** is used.
- If a sequence number is not provided, the sequence number is incremented by 10 automatically.
- If a matching statement is not included, an implied all prefixes is associated with the statement.
- Processing within a route map stops after all optional actions have processed and after matching a conditional matching criterion.

17. A company is deploying BGP multihoming to provide network connection redundancy for several branch sites. Which method can be used to avoid the branch transit routing situation?

- ensuring that no IGP session is running on branch site BGP routers
- designating a data center or a specific location to handle the transit traffic
- applying inbound BGP route policies so that only data packets from other branch sites can enter local networks
- **applying outbound BGP route policies so that** branch sites do not advertise routes learned from the WAN connection

Explanation: Multihomed environments should be configured so that branch routers cannot act as transit routers. In most designs, transit routing of traffic from another branch is undesirable, because WAN bandwidth may not be sized accordingly. Transit routing can be avoided by configuring outbound route filtering at each branch site so that the branch sites do not advertise what they learn from the WAN but advertise only networks that face the LAN.

18. A BGP routing policy has been created using route maps. The command `route-map TEST permit 10` is part of the configuration. What does the argument 10 indicate?

- It identifies the access list number to be used by the route map statement.
- **It identifies the position of the route map in relation to other instances.**
- It indicates the local preference to be set for routes that match the route map.
- It indicates the metric to be set for routes that match the route map.
- It specifies the route map to be used on autonomous system 10.

Explanation: A route map uses the command syntax **route-map** *route-map-name* [**permit** | **deny**][*sequence-number*]. It has four components:

- **Sequence number** – dictates the processing order of the route map
- **Conditional matching criteria** – identifies prefix characteristics (network, BGP path attribute, next hop, and so on) for a specific sequence
- **Processing action** – permits or denies the prefix
- **Optional action** – allows for manipulations, depending on how the route map is referenced on the router

19. A network administrator is configuring an ACL to match networks for BGP route filtering. The administrator creates an ACE permit ip 10.0.128.0 0.0.63.0 255.255.255.0 0.0.0.0. Which network matches the ACE?

- 10.0.63.0/24
- **10.0.130.0/24**
- 10.0.192.0/24
- 10.0.128.0/25

Explanation: One method for conditional matching of routes in BGP is through extended ACLs. When using extended ACLs for this purpose, the source fields match against the network portion of the route, and the destination fields match against the network mask. The matching networks are 10.0.128.0/24 through 10.0.191.0/24.

20. A network administrator is configuring a prefix list to match networks for BGP route filtering. Which network matches the prefix match specification 10.160.0.0/14 ge 22?

- 10.158.0.0/22
- 10.162.0.0/14
- **10.163.0.0/24**
- 10.128.0.0/28

Explanation: Prefix lists provide another method of identifying networks in a routing protocol. A prefix list identifies a specific IP address, network, or network range and allows for the selection of multiple networks with a variety of prefix lengths by using a prefix match specification. A prefix match specification contains two parts: a high-order bit pattern and a high-order bit count, which determines the high-order bits in the bit pattern that are to be matched. The high-order bit pattern is also known as the network address and the high-order bit count as the mask length. The network portion of the matching networks is 10.160.0.0 and higher. The mask length of the matching networks must be greater than or equal to /22.

21. Refer to the exhibit. A network administrator is troubleshooting BGP configuration and wants to verify routes that carry the 100 AS in the AS_Path value. Which regular expression should the administrator use in the command show bgp ipv4 unicast regex regex-pattern?

```
R1# show bgp ipv4 unicast

<Output omitted>

      Network           Next Hop       Metric LocPrf Weight Path
*> 172.16.0.0/24      192.168.200.3      0               0 300 80 90 21003 2100 i
*> 172.16.4.0/23      192.168.200.3      0               0 300 1080 1090 1100 1110 i
*> 172.16.16.0/22     192.168.200.3      0               0 300 11234 21234 31234 i
*> 172.16.99.0/24     192.168.200.3      0               0 300 40 i
*> 172.16.129.0/24    192.168.200.3      0               0 300 10010 30010 30050 i
*>i192.168.0.0        10.12.1.1          0     100       0 100 80 90 21003 2100 i
*>i192.168.4.0/23     10.12.1.1          0     100       0 100 1080 1090 1100 1110 i
*>i192.168.16.0/22    10.12.1.1          0     100       0 100 11234 21234 31234 i
*>i192.168.99.0       10.12.1.1          0     100       0 100 40 i
*>i192.168.129.0      10.12.1.1          0     100       0 100 10010 300 30010 30050 i
```

- show bgp ipv4 unicast regex .100.
- show bgp ipv4 unicast regex $100
- **show bgp ipv4 unicast regex 100_**
- show bgp ipv4 unicast regex ^100^

Explanation: In troubleshooting BGP, regular expressions (regex) can be used to parse through the large number of available ASNs. Regular expressions are based on query modifiers used to select the appropriate content. The regex pattern 100_ indicates to only include the lines that contain the exact phrase of 100. Some regex query modifiers are as follows:

- (underscore) – Matches a space

- ^ (caret) – Indicates the start of a string
- $ (dollar sign) – Indicates the end of a string
- . (period) – Matches a single character, including a space

22. What is the first attribute to be used in determining the best path when a BGP router has multiple paths for the same network prefix length?

- **weight**
- lowest MED
- local originated
- local preference

Explanation: The BGP best-path algorithm uses the attributes, in the following order, for the best-path selection:

1. Weight.
2. Local preference.
3. Local originated (network statement, redistribution, or aggregation).
4. AIGP.
5. Shortest AS_Path.
6. Origin type.
7. Lowest MED.
8. EBGP over IBGP.
9. Lowest IGP next hop.
10. If both paths are external (EBGP), prefer the first (oldest).
11. Prefer the route that comes from the BGP peer with the lower RID.
12. Prefer the route with the minimum cluster list length.
13. Prefer the path that comes from the lowest neighbor address.

23. Refer to the exhibit. A network administrator is configuring BGP route filtering on R1. The router ID for R1 is configured with lookback address 192.168.1.1. Which three routes are allowed from the BGP neighbor router 10.12.1.2 to inject into the BGP table of R1? (Choose three.)

```
R1

ip access-list extended ACL-IN
 permit ip 192.168.0.0 0.0.255.255 host 255.255.255.255
 permit ip 64.100.0.0 0.0.255.0 host 255.255.255.128
 !
router bgp 65100
  address-family ipv4
    neighbor 10.12.1.2 distribute-list ACL-IN in
```

- 192.168.1.1/32
- **192.168.2.2/32**
- **192.168.3.3/32**
- 10.12.1.0/24
- **64.100.3.0/25**
- 64.100.2.192/26

Explanation: Per the distribute list filtering ACL-IN, two loopback networks (192.168.2.2/32 and 192.168.3.3/32) are allowed because they match the first ACE in the ACL-IN. The network 64.100.3.0/25 is allowed because it matches the second ACE in the ACL-IN. The networks 192.168.1.1/32 and 10.12.1.0/24 are local routes. The network 64.100.2.192/26 would not be allowed because it does not match entries in the ACL-IN.

24. A network administrator is configuring a prefix list with the `ip prefix-list` command. How does the IOS process the prefix list if the administrator does not specify a sequence number?

- It will present a prompt to ask the administrator to enter one.
- It will present an error message that indicates the entry fails.
- **It automatically increments by 5 based on the highest sequence number.**
- It automatically increments by 10 based on the highest sequence number.

Explanation: Prefix lists are configured with the global configuration command **ip prefix-list** *prefix-listname* [**seq** *sequence-number*] {**permit** | **deny**} *high-order-bit-pattern/high-order-bit-count* [**ge** *ge-value*][**le** *le-value*]. If a sequence is not provided, the sequence number automatically increments by 5 based on the highest sequence number.

1. IGMP snooping examines traffic at which OSI layer(s)?

- Layer 2
- Layer 3
- **Layer 2 and Layer 3**
- Layer 2, Layer 3, and Layer 4

Explanation: IGMP snooping examines traffic at layer two for unicast traffic and layer three for multicast traffic.

2. An IPv6 enabled device sends a data packet with the destination address of FF02::1. What is the target of this packet?

- all IPv6 DHCP servers
- **all IPv6 enabled nodes on the local link**
- all IPv6 configured routers on the local link
- all IPv6 configured routers across the network

Explanation: FF02::1 is the all-nodes multicast group within the scope of the local link. A packet with this destination address is received and processed by all IPv6-enabled interfaces.

3. What is the hexadecimal representation of the first 24 bits of any multicast MAC address?

- **01:00:5E**
- 00:E1:12
- 01:5E:01
- 00:1E:12

Explanation: The first 24 bits of a multicast MAC address are always 01:00:5E.

4. What is the IP address for the Cisco-RP-discovery multicast group?

- 224.0.0.1
- 224.0.1.39
- **224.0.1.40**
- 224.1.1.1

Explanation: The multicast address 224.0.1.40 is the address used by RP MAs to advertise the RP mappings to another well-known multicast group.

5. Which IP address does the BSR mechanism use to send all BSR messages?

- 224.0.0.10
- 224.0.0.14
- 224.0.0.15
- **224.0.0.13**

Explanation: BSR messages are sent by the bootstrap router mechanism using the IP address 224.0.0.13 with a TTL factor of one.

6. What is the default maximum response time for a general membership query message sent to the all-host group address 224.0.0.1 in an attached subnet?

- 5 seconds
- 8 seconds
- **10 seconds**
- 12 seconds

Explanation: The general query message has a default max response time field that is set to 10 seconds. However, this can be set using a nondefault value.

7. Which version of IGMP supports Source Specific Multicast (SSM)?

- IGMPv1
- IGMPv2
- **IGMPv3**

Explanation: The PIM extension Source Specific Multicast (SSM) is supported only by IGMPv3.

8. What message type would a receiver in a multicast environment send in order to receive a specific multicast feed?

- IGMP include
- IGMP exclude
- **IGMP join**
- IGMP Version 2 specific query

Explanation: The Internet Group Management Protocol (IGMP) is a protocol used by receivers to join multicast groups. This is done by using the IGMP join membership report.

9. What is a benefit of shared trees over source trees when comparing multicast distribution trees?

- Shared trees receive traffic from all sources that send traffic to the multicast group.
- **They require fewer multicast entries.**
- They can allow multiple sources in an IP multicast group.
- They can be pruned.

Explanation: Shared trees receive traffic from all sources sending traffic to the same multicast group. This generates a lot of unnecessary traffic. However, because they use Rendezvous Points, shared trees require fewer multicast entries.

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

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

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.

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

- PIM does not require an IGP protocol to be configured in the network.
- PIM should be configured only on the first and the last hop routers in the multicast tree.
- 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 is a multicast routing protocol that makes packet-forwarding decisions independent of the unicast IP routing protocol that is running in the network.**
- **Three of the forwarding modes for PIM are PIM dense mode (PIM-DM), PIM sparse mode (PIMSM), and PIM sparse-dense mode.**

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)

12. For configuring IP multicast routing, what is the purpose of the global configuration mode command `ip pim send-rp-announce 10.1.1.1` ?

- enables IP multicast routing with router ID 10.1.1.1
- assigns the role of rendezvous point mapping agent to the router with IP address 10.1.1.1
- **announces the candidacy of the router with IP address 10.1.1.1 as the rendezvous point for all multicast groups**
- enables protocol independent multicast (PIM) with router ID 10.1.1.1

Explanation: The command `ip pim send-rp-announce 10.1.1.1` is used in Auto-RP to announce the candidacy of the router with IP address 10.1.1.1 as the rendezvous point for all multicast groups. This command is used in the global configuration mode.