DumpsCafe

Fortinet

NSE6_FSW-7.2

NSE6_FSW-7.2 - Fortinet NSE 6 - FortiSwitch 7.2

Version: Demo

[Total Questions: 10]

Web: www.dumpscafe.com

Email: support@dumpscafe.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpscafe.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@dumpscafe.com and our technical experts will provide support within 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

Question #:1

Which Ethernet frame can create Layer 2 flooding due to all bytes on the destination MAC address being set to all FF?

A. The broadcast Ethernet frame

B. The unicast Ethernet frame

C. The multicast Ethernet frame

D. The anycast Ethernet frame

Answer: A

Explanation

Layer 2 flooding caused by Ethernet frames with all bytes in the destination MAC address set to FF refers to broadcast frames. Here’s why:

- **Broadcast Ethernet Frame (A):**
  - **Address Specification:**In Ethernet networking, a broadcast frame has a destination MAC address of**FF:FF:FF:FF:FF:FF**, which instructs network devices to forward the frame to all devices within the broadcast domain.
  - **Network Behavior:**This causes Layer 2 flooding as the frame is sent to all ports in the VLAN, except the originating port, ensuring that the broadcast reaches all network segments.
- **Other Frame Types:**
  - **Unicast (B)**targets a single device.
  - **Multicast (C)**targets a group of devices.
  - **Anycast (D)**is not used in Ethernet but rather in IP-based routing to route to the nearest of multiple destinations, typically in internet addressing.

References: You can find more information about Ethernet frame types in networking textbooks or documentation that discusses network layer interaction:Network Theory Books

Question #:2

Which statement about the IGMP snooping querier when enabled on a VLAN is true?

A. Active multicast receiver entries are aging on each IGMP query sent on the VLAN

B. IGMP reports on the VLAN are forwarded to all switch ports.

C. The setting can only be enabled using the FortiSwitch CLI.

D. All other indirectly connected switches will be unable to get IGMP multicast traffic.

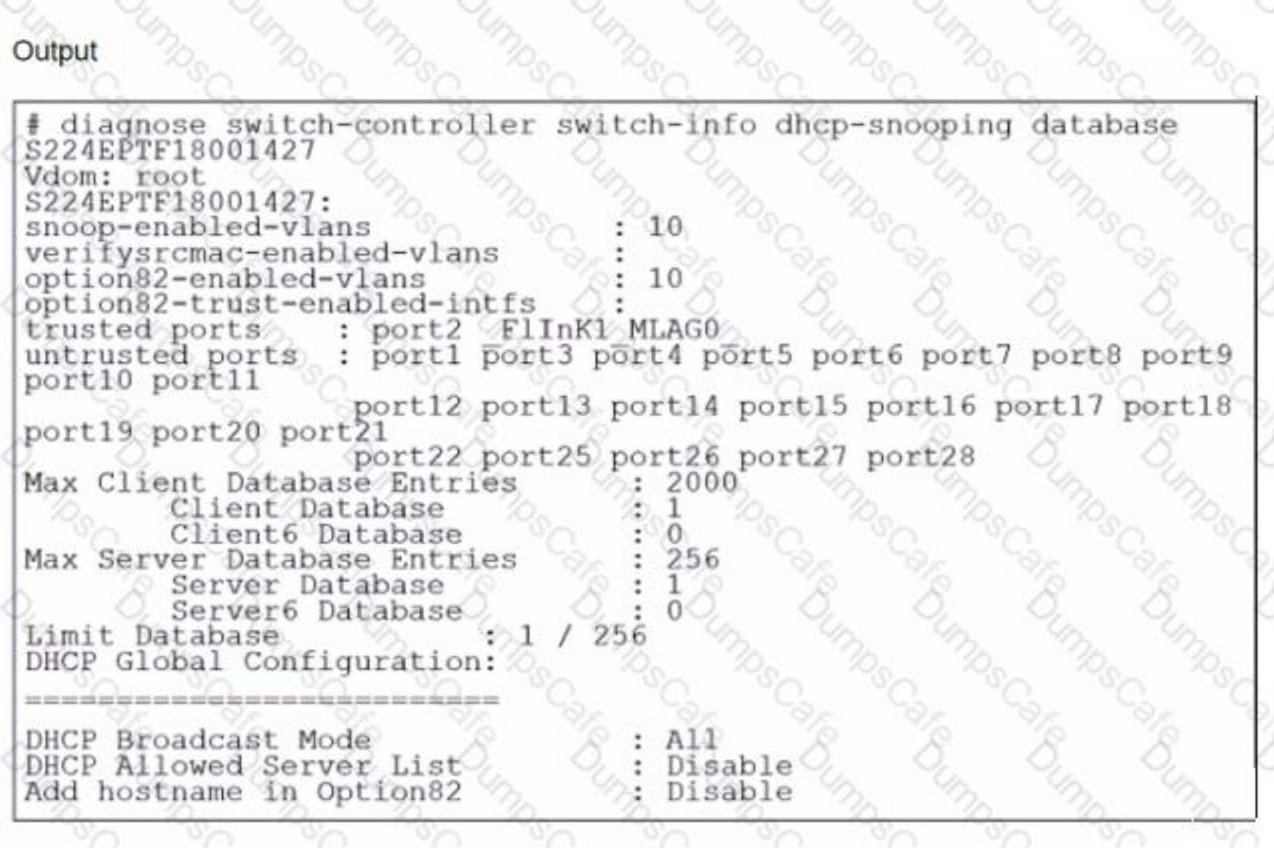
Answer: A

Explanation

Active multicast receiver entries are aging on each IGMP query sent on the VLAN (A): When IGMP snooping querier is enabled on a VLAN, it functions to manage multicast traffic within the VLAN by keeping track of multicast group memberships. The IGMP querier sends queries to determine which ports require the multicast traffic. The multicast receiver entries, which are entries that indicate which devices have requested the multicast data, age or time out based on these IGMP queries. Each query refreshes active connections but ages out entries that no longer respond, helping to ensure that multicast traffic is only sent to ports with active receivers.

Question #:3

Refer to the exhibit.



Output

```
# diagnose switch-controller switch-info dhcp-snooping database
S224EPTF18001427
Vdom: root
S224EPTF18001427:
snoop-enabled-vlans               : 10
verifysrcmac-enabled-vlans        :
option82-enabled-vlans            : 10
option82-trust-enabled-intfs      :
trusted ports     : port2  FlInK1 MLAG0
untrusted ports   : port1 port3 port4 port5 port6 port7 port8 port9
port10 port11
                   port12 port13 port14 port15 port16 port17 port18
port19 port20 port21
                   port22 port25 port26 port27 port28
Max Client Database Entries        : 2000
       Client Database             : 1
       Client6 Database            : 0
Max Server Database Entries        : 256
       Server Database             : 1
       Server6 Database            : 0
Limit Database             : 1 / 256
DHCP Global Configuration:
==========================
DHCP Broadcast Mode                : All
DHCP Allowed Server List           : Disable
Add hostname in Option82           : Disable
```

What two conclusions can be made regarding DHCP snooping configuration? (Choose two.)

A. Maximum value to accept clients DHCP request is configured as per DHCP server range.

B. FortiSwitch is configured to trust DHCP replies coming on FortiLink interface.

C. DHCP clients that are trusted by DHCP snooping configured is only one.

D. Global configuration for DHCP snooping is set to forward DHCP client requests on all ports in the VLAN.

Answer: B D

Explanation

Based on the DHCP snooping configuration details provided in the exhibit:

- B. FortiSwitch is configured to trust DHCP replies coming on FortiLink interface.The configuration segment shows "trusted ports : port2 FlInK1 MLAG0," indicating that the FortiSwitch is configured to trust DHCP replies coming from the specified ports, including the FortiLink interface labeled FlInK1. This setup is critical in environments where the FortiLink interface connects directly to a trusted device, such as a FortiGate appliance, ensuring that DHCP traffic on these ports is considered legitimate.

- D. Global configuration for DHCP snooping is set to forward DHCP client requests on all ports in the VLAN.The "DHCP Broadcast Mode" set to 'All'under the DHCP Global Configuration indicates that DHCP client requests are allowed to broadcast across all ports within the VLAN. This setting is essential for environments needing broad DHCP client servicing across multiple access ports without restriction, facilitating network connectivity and management.

Question #:4

Which LLDP-MED Type-Length-Values does FortiSwitch collect from endpoints to track network devices and determine their characteristics?

A. Network policy

B. Power management

C. Location

D. Inventory management

Answer: D

Explanation

While FortiSwitch can collect all the listed LLDP-MED TLVs (Network Policy, Power Management, Location, and Inventory Management), the primary focus for tracking and identifying network devices is on the**Inventory Management**TLV.

This TLV carries critical details such as:

- Manufacturer

- Model

- Hardware/Firmware versions
- Serial/Asset numbers

This information provides a granular understanding of the devices on your network.

Question #:5

What are two reasons why time synchronization between FortiGate and its managed FortiSwitch is critical in switch management? (Choose two.)

A. FortiSwitch does not retain its time after a reboot, which gets reset after each reboot.

B. FortiSwitch will not be able to become an NTP server for downstream devices.

C. FortiSwitch cannot complete the DTLS handshake used in the CAPWAP tunnel.

D. FortiSwitch will not allow other FortiSwitch devices in the chain be discovered by FortiGate.

Answer: A C

Explanation

Time synchronization between FortiGate and its managed FortiSwitch devices is essential for several reasons:

- A. FortiSwitch does not retain its time after a reboot, which gets reset after each reboot.This characteristic of FortiSwitch underlines the importance of time synchronization with FortiGate. Since FortiSwitch loses its time settings upon reboot, synchronizing with FortiGate ensures that its system clock is accurate, which is vital for logging, troubleshooting, and security timestamping.
- C. FortiSwitch cannot complete the DTLS handshake used in the CAPWAP tunnel.Accurate time synchronization is crucial for security protocols such as DTLS, which rely on timestamped certificates for establishing a secure connection. If the time on FortiSwitch is not synchronized with FortiGate, the DTLS handshake used in the CAPWAP tunnel for secure communication may fail due to time discrepancies, impacting the management and operation of the switch.

Question #:6

Which two statements about the FortiLink authorization process are true? (Choose two.)

A. The administrator must manually pre-authorize FortiGate on FortiSwitch by adding the FortiGate serial number.

B. FortiSwitch requires a reboot to complete the authorization process.

C. A FortiLink frame is sent by FortiGate to FortiSwitch to complete the authorization.

D. FortiLink authorization sets the FortiSwitch management mode to FortiLink.

Answer: C D

Explanation

The FortiLink authorization process is an integral part of setting up FortiSwitch to be managed by FortiGate. The correct statements regarding the FortiLink authorization process are:

C.**A FortiLink frame is sent by FortiGate to FortiSwitch to complete the authorization.**This is a part of the FortiLink protocol, where FortiGate communicates with the connected FortiSwitch to establish management and control. This frameinitiates the configuration and management process, allowing FortiGate to effectively control the switch.

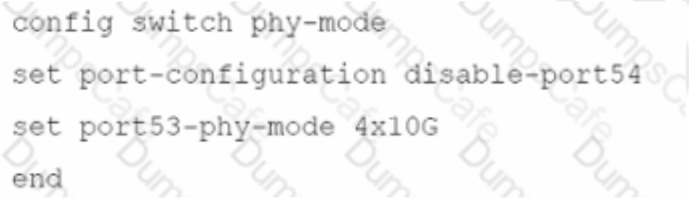
D.**FortiLink authorization sets the FortiSwitch management mode to FortiLink.**Once authorized, the management mode of FortiSwitch is set to FortiLink, indicating that it is being managed via a FortiLink connection from a FortiGate appliance. This changes the operational mode of the switch to be under the control of the FortiGate for centralized management and policy application.

References:

- Further details on the FortiLink setup and authorization process can be accessed through the FortiGate configuration guides available on theFortinet Documentation site.

Question #:7

Refer to the configuration:



```
config switch phy-mode
set port-configuration disable-port54
set port53-phy-mode 4x10G
end
```

Which two conditions does FortiSwitch need to meet to successfully configure the options shown in the exhibit above? (Choose two.)

A. The FortiSwitch model is equipped with a maximum of 54 interfaces

B. FortiSwitch would need to be rebooted.

C. The split port can be assigned to a native VLAN.

D. The Dort full speed prior to the split was 100G QSFP+.

Answer: A B

Question #:8

How does FortiSwitch perform actions on ingress and egress traffic using the access control list (ACL)?

A. Only high-end FortiSwitch models support ACL.

B. ACL can be used only at the prelookup stage in the traffic processing pipeline.

C. Classifiers enable matching traffic based only on the VLAN ID.

D. FortiSwitch checks ACL policies only from top to bottom.

Answer: D

Explanation

In FortiSwitch, Access Control Lists (ACLs) are used to enforce security rules on both ingress and egress traffic:

- **ACL Evaluation Order (D):**
  - **Operational Function:**FortiSwitch processes ACL entries from top to bottom, similar to how firewall rules are processed. The first match in the ACL determines the action taken on the packet, whether to allow or deny it, making the order of rules critical.
  - **Configuration Advice:**Careful planning of the order of ACL rules is necessary to ensure that more specific rules precede more general ones to avoid unintentional access or blocks.

References: For a comprehensive guide on configuring ACLs in FortiSwitch, consult the FortiSwitch security settings documentation available on:Fortinet Product Documentation

Question #:9

Which QoS mechanism maps packets with specific CoS or DSCP markings to an egress queue?

A. Queuing for egress traffic

B. Classification for ingress traffic

C. Rate limiting for egress traffic

D. Marking for ingress traffic

Answer: B

Explanation

"Classification: FortiSwitch maps packets with a given CoS or DSCP marking to an egress queue. There are eight egress queues on each port: queues 0 to 7."

In Quality of Service (QoS) mechanisms, the process of mapping packets with specific CoS (Class of Service) or DSCP (Differentiated Services Code Point) markings to an egress queue involves two key steps: **classification**and**queuing**.

- **Classification**: This occurs on the ingress side (incoming traffic). The switch examines the packet headers (e.g., CoS or DSCP values) to determine how the traffic should be treated. Based on this classification, the switch assigns the packet to a specific priority level or queue.

- **Queuing**: Once the packet is classified, it is mapped to an egress queue based on its priority level. The egress queues are used to manage how traffic is transmitted out of the switch.

- **Option A (Queuing for egress traffic)**refers to managing how packets leave the switch, but it does not involve the initial mapping of CoS/DSCP values to a queue.

- **Option C (Rate limiting for egress traffic)**is about controlling the rate of outgoing traffic, which is unrelated to CoS/DSCP mapping.

- **Option D (Marking for ingress traffic)**involves modifying the CoS or DSCP values of packets as they enter the switch, but it does not map them to an egress queue.

Thus,**classification for ingress traffic**is the mechanism that identifies and maps packets with specific CoS or DSCP markings to an appropriate egress queue.

Question #:10

What feature can network administrators use to segment network operations and the administration of managed FortiSwitch devices on FortiGate?

A. FortiGate multi-tenancy

B. Multi-chassis link aggregation trunk

C. FortiGate clustering protocol

D. FortiLink split interface

Answer: A

Explanation

FortiGate's multi-tenancy feature, specifically Virtual Domains (VDOMs), is the most appropriate tool for segmenting network operations and the administration of managed FortiSwitch devices on FortiGate. Here's why:

- VDOMs as Virtual Firewalls:VDOMs function as independent virtual firewalls within a single FortiGate device. Each VDOM can have its own:
  - Security policies
  - Interfaces (Including FortiLink interfaces for FortiSwitch management)
  - Routing table
  - Administrative access

- Segmenting Network Operations:By assigning different FortiSwitch devices (or groups of ports) to separate VDOMs, you effectively partition your network. Network administrators can manage specific FortiSwitches through their assigned VDOMs, maintaining operational isolation.

- Enhanced Administration:VDOMs offer granular administrative control. Different administrators can be assigned to specific VDOMs, limiting their management scope and reducing the risk of accidental configuration changes.

Why Other Options Are Less Suitable:

- B. Multi-chassis link aggregation trunk:This focuses on link redundancy and bandwidth aggregation, not network segmentation.

- C. FortiGate clustering protocol:This is aimed at high availability and scalability of the firewall functions themselves, not the management of switches.

- D. FortiLink split interface:This allows dividing a FortiLink interface on the FortiGate for managing multiple FortiSwitches, but it doesn't provide the true segmentation and administrative isolation that VDOMs offer.

References:

- Fortinet Document Library - VDOMs:[invalid URL removed]

- Fortinet Document Library - FortiSwitch Multi-tenancy (using VDOMS):https://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/801172/multitenancy-and-vdoms

About dumpscafe.com

dumpscafe.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@dumpscafe.com
- Feedback: feedback@dumpscafe.com
- Support: support@dumpscafe.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.