Number: NSE6_FSW-7.2
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: NSE6_FSW-7.2

Exam Name: Fortinet NSE 6 - FortiSwitch 7.2

Exam A

QUESTION 1
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

Correct Answer: D
Section:

QUESTION 2
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.

Correct Answer: B, C
Section:

QUESTION 3
FortiGate is unable to establish a tunnel with the FortiSwitch device it is supposed to manage Based on the debug output shown in the exhibit, what is the reason for the failure?

A. The handshake process timed out before FortiSwitch responded.
B. DTLS client hello had the incorrect pre-shared key.
C. The CAPWAP tunnel failed to come up due to a mismatch in time.
D. FortiSwitch has disabled FortiLink and is only managed as a standalone.

Correct Answer: C
Section:

QUESTION 4
Refer to the exhibit.
The profile shown in the exhibit is assigned to a group of managed FortiSwitch ports. and these ports are connected to endpoints which are powered by PoE. Which configuration action can you perform on the LLDP profile to cause these endpoints to exchange PoE information and negotiate power with the managed FortiSwitch?

A. Assign a new LL0P profile to handle different LLDP-ME0 TLVs
B. Add power management as part of LLDP-MED TLVs to advertise.
C. Define an LLDP-ME0 location 10 to use standard protocols for power.
D. Create new a LLOP-MEO application type to define the PoE parameters.

Correct Answer: B
Section:

QUESTION 5
What can an administrator do to maintain the existing standalone FortlSwltch configuration while changing the management mode to FortLink?

A. Use a migration tool based on python script to convert the configuration
B. Enable the Forti-link setting on FortiSwitch before the authorization process
C. FortiGate will automatically save the existing FortiSwitch configuration during the Forti-link management process.
D. Register FortiSwitch to For1ISwitch Cloud to save a copy before managing by Forti-Gate.

Correct Answer: B
Section:

QUESTION 6
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.

Correct Answer: A, C
Section:

QUESTION 7

Which statement about the quarantine VLAN on FortiSwitch is true?

A. Quarantine VLAN has no DHCP server
B. Users who fail 802.1X authentication can be placed on the quarantine VLAN.
C. It is only used for quarantined devices if global setting is set to quarantine by VLAN.
D. FortiSwitch can block devices without configuring quarantine VLAN to be part of the allowed VLANs.

Correct Answer: C
Section:

QUESTION 8
Which packet capture method allows FortiSwitch to capture traffic on trunks and management interfaces?

A. SPAN
B. Sniffer profile
C. sFlow
D. TCP dump

Correct Answer: C
Section:

QUESTION 9
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

Correct Answer: A
Section:

QUESTION 10
Which is a requirement to enable SNMP v2c on a managed FortiSwitch?

A. Create an SNMP user to use for authentication and encryption.
B. Specify an SNMP host to send traps to.
C. Enable an SNMP v3 to handle traps messages with SNMP hosts.
D. Configure SNMP agent and communities.

Correct Answer: D
Section:

QUESTION 11
Refer to the diagnostic output:

```
# diagnose switch-controller switch-info mac-table
Vdom: root
S224EPTF19005928 0 :
MAC address Interface vlan
=====================================================
04:d5:90:39:73:3d internal 4092
04:d5:90:3e:e2:88 port1 4089
00:50:56:96:e3:fc GVM1V0000141680 4089
04:d5:90:39:73:3d internal 4094
00:50:56:96:e3:fc GVM1V0000141680 4094
```

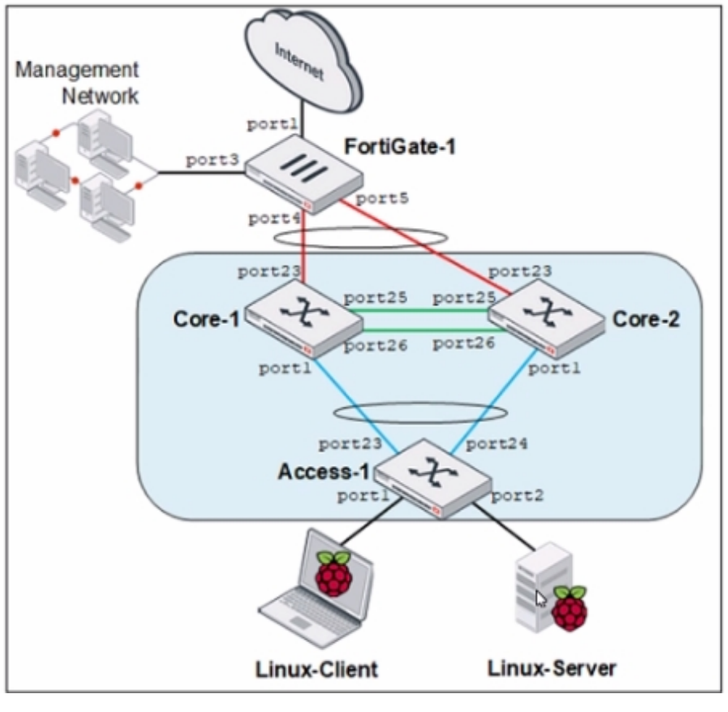
Two entries in the exhibit show that the same MAC address has been used in two different VLANs. Which MAC address is shown in the above output?

A. It is a MAC address of FortiLink interface on FortiGate.
B. It is a MAC address of a switch that accepts multiple VLANs.
C. It is a MAC address of an upstream FortiSwitch.
D. It is a MAC address of FortiGate in HA configuration.

Correct Answer: B
Section:

QUESTION 12
Refer to the exhibit.

MCL-Topology



Core-1 and Access-1 are managed and authorized by FortiGate-1. which uses port4 as the FortiLink interface. After FortiGate authorizes and manages Core-2. Port1 status becomes STP discarding.
Why is port1 in the discarding state?

A. port1 on Core-2 is discarding only management traffic.
B. Core-1 and Core-2 do not have MCLAG configuration.
C. Access-1 is the root bridge and can only have one root port.
D. Core-2 has the lowest bridge priority.

Correct Answer: B
Section:

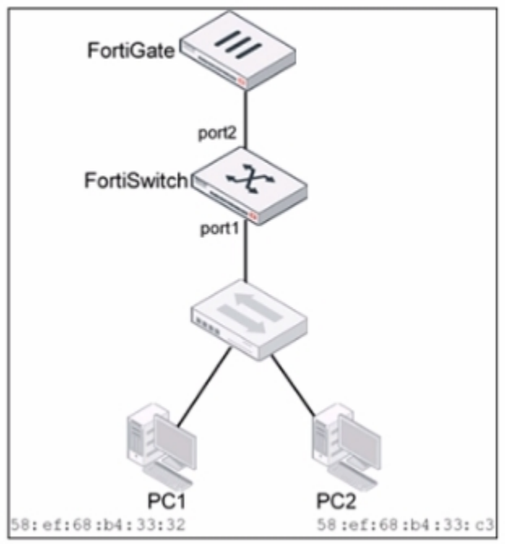
QUESTION 13
Which two statements about the FortiLink authorization process are true? (Choose two.)

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.

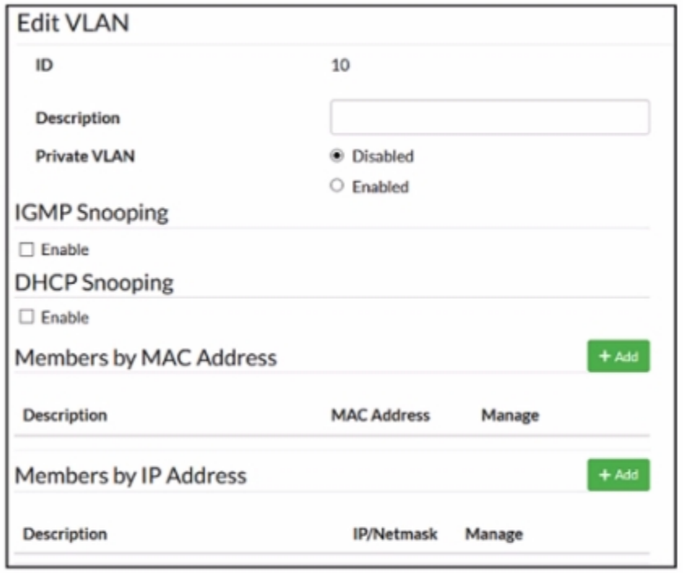
Correct Answer: C, D
Section:

QUESTION 14
Refer to the exhibits

Topology



VLAN



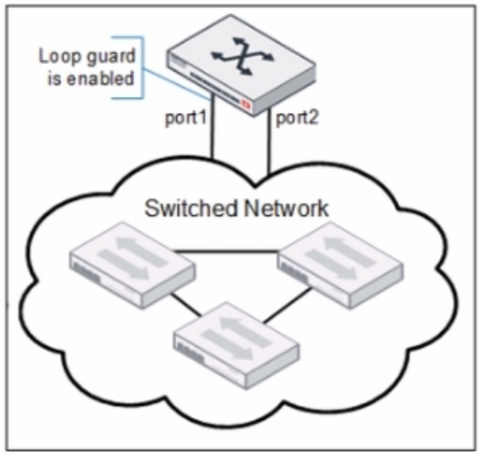
Traffic arriving on port2 on FortiSwitch is tagged with VLAN ID 10 and destined for PC1 connected on port1. PC1 expects to receive traffic untagged from port1 on FortiSwitch.
Which two configurations can you perform on FortiSwitch to ensure PC1 receives untagged traffic on port1? (Choose two.)

A. Add the MAC address of PCI as a member of VLAN 10.
B. Add VLAN ID 10 as a member of the untagged VLANs on port1.
C. Remove VLAN 10 from the allowed VLANs and add it to untagged VLANs on port1.
D. Enable Private VLAN on VLAN 10 and add VLAN 20 as an isolated VLAN.

Correct Answer: A, B
Section:

QUESTION 15
Refer to the exhibits.

LoopGuard-setup



LoopGuard-setup

```
# diagnose switch-controller switch-info loop-guard S108EF4N17000029
S108EF4N17000029:
  Portname            State     Status      Timeout(m)   MAC-Move   Count   Last-Event
  ________________    _______   _________   __________   ________   _____   ___________________
  port1               enabled   Triggered       2            0        1    2021-02-19 15:50:35
  port2               disabled    -             -            -        -          -
  port3               disabled    -             -            -        -          -
  port4               disabled    -             -            -        -          -
  port5               disabled    -             -            -        -          -
  port6               disabled    -             -            -        -          -
  port9               disabled    -             -            -        -          -
  port10              disabled    -             -            -        -          -
  8EF4N17000030-0     disabled    -             -            -        -          -
  _FlInK1_MLAG0_      disabled    -             -            -        -          -
```

Port1 and port2 are the only ports configured with the same native VLAN 10.
What are two reasons that can trigger port1 to shut down? (Choose two.)

A. port1 was shut down by loop guard protection.
B. STP triggered a loop and applied loop guard protection on port1.
C. An endpoint sent a BPDU on port1 that it received from another interface.
D. Loop guard frame sourced from port 1 was received on port 1.

Correct Answer: B, C
Section:

QUESTION 16
Refer to the diagnostic output:

```
# diagnose sniffer packet __port__23 "" 4
interfaces=[__port__23]
filters=[]
pcap_lookupnet: __port__23: no IPv4 address assigned
2.100771 __port__23 -- 802.1Q vlan#4094 P0 -- Ether type 0x79 printer havn't been added to sniffer
2.188294 __port__23 -- 802.1Q vlan#4094 P0 -- lldp 194 chassis 4 04:d5:90:c2:fa:d4 port subtype 5: 'port1' ttl 120 system 'Core-
1'
```

What makes the use of the sniffer command on the FortiSwitch CLI unreliable on__port__23?

A. The types of packets captured is limited.
B. Just the port egress payloads are printed on CLI.
C. Only untagged VLAN traffic can be captured.
D. The switch port might be used as a trunk member

Correct Answer: A
Section:

QUESTION 17
Which interfaces on FortiSwitch send out FortiLink discovery frames by default in order to detect a FortiGate with an enabled FortiLink interface?

A. All ports have auto-discovery enabled by default.
B. No ports are enabled by default for auto-discovery. This must be configured under config switch interface.
C. The ports with auto-discovery enabled by default are dependent upon the FortiSwitch model.
D. The last four switch ports on FortiSwitch have auto-discovery enabled by default.

Correct Answer: A
Section:

QUESTION 18
Refer to the exhibit.

Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping
Access-1 - S424DPTF20000029 (4)								
port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered	00:e0:4c:36:0e:a6	Untrusted
port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered	5c:85:7e:32:16:a2	Untrusted
port23		Normal	Edge Port Spanning Tree Protocol	S424DPTF20000027		Powered		

The exhibit shows the current status of the ports on the managed FortiSwitch. Access-1.
Why would FortiGate display a serial number in the Native VLAN column associated with the port23 entry?

A. port23 is configured as the dedicated management interface.
B. Ports connected to adjacent FortiSwitch devices show their serial number as the native VLAN.
C. port23 is a member of a trunk that uses the Access-1 FortiSwitch serial number as the name of the trunk.
D. A standalone switch with the shown serial number is connected on port23.

Correct Answer: D
Section:

QUESTION 19
What are two ways in which automatic MAC address quarantine works on FortiSwitch? (Choose two.)

A. FortiSwitch supports only by VLAN quarantine mode.
B. FortiGate applies the quarantine-related configuration only on FortiGate.
C. FortiAnalyzer with a threat detection services license is required.
D. MAC address quarantine can be enabled through the FortiGate CLI only.

Correct Answer: C, D
Section:

QUESTION 20
What can an administrator do to maintain a FortiGate-compatible FortiSwitch configuration when changing the management mode from standalone to FortiLinK?

A. Use a migration tool based on Python script to convert the configuration.
B. Enable the FortiLink setting on FortiSwitch before the authorization process.
C. FortiGate automatically saves the existing FortiSwitch configuration during the FortiLink management process.
D. Register FortiSwitch to FortiSwitch Cloud to save a copy before managing with FortiGate.

Correct Answer: D
Section:

QUESTION 21
Refer to the exhibit.
Output

```
2021-07-23 12:13:19 573s:160ms:74us flp_event_handler[734]:node: port4
received event 101 state FL_STATE_WAIT_JOIN switchname S424DPTF20000029
flags 0x401
2021-07-23 12:13:21 575s:396ms:114us flp_event_handler[734]:node: port4
received event 110 state FL_STATE_READY switchname  flags 0x124a
2021-07-23 12:13:21 575s:398ms:724us flp_event_handler[734]:node: port4
received event 111 state FL_STATE_READY switchname  flags 0x124a
2021-07-23 12:13:21 575s:403ms:607us flp_send_pkt[445]:pkt-sent (type(5)
flag=0x18ca node(port4) sw(port4) len(26)smac: 0:50:56:96:d8: 2 dmac:
4:d5:90:c2:fa:ea
2021-07-23 12:13:22 576s:284ms:825us flp_send_pkt[445]:pkt-sent (type(3)
flag=0x8a node(port4) sw(S424DPTF20000029) len(26)smac: 0:50:56:96:d8: 2
dmac: 4:d5:90:c2:fb: b
2021-07-23 12:13:24 578s:411ms:316us flp_event_handler[734]:node: port4
received event 110 state FL_STATE_READY switchname  flags 0x124a
2021-07-23 12:13:24 578s:413ms:151us flp_event_handler[734]:node: port4
received event 111 state FL_STATE_READY switchname  flags 0x124a
2021-07-23 12:13:24 578s:415ms:255us flp_send_pkt[445]:pkt-sent (type(5)
flag=0x18ca node(port4) sw(port4) len(26)smac: 0:50:56:96:d8: 2 dmac:
4:d5:90:c2:fa:ea
```

Which two statements best describe what is displayed in the FortiLink debug output shown in the exhibit? (Choose two.)

A. FortiSwitch is sending FortiLink heartbeats to FortiGate.
B. FortiSwitch is discovered and authorized by FortiGate.

C. FortiSwitch is in a waiting state to join the stack group on FortiGate.
D. FortiSwitch is ready to push its new hostname to FortiGate.

Correct Answer: A, B
Section:

QUESTION 22
Which two statements about VLAN assignments on FortiSwitch ports are true? (Choose two.)

A. Configure a native VLAN on the FortiLink
B. Assign an IP address and subnet mask to FortiSwitch VLANs
C. Only assign one native VLAN on a port
D. Assign untagged VLANs using FortiGate CLI

Correct Answer: C, D
Section:

QUESTION 23
Which two rules used by MSTP are similar to rules used by other STP methods? (Choose two.)

A. MSTP uses port role election, similar to rapid STP on the instances.
B. MSTP uses alternate path and primary path, similar to regular STP.
C. MSTP uses root bridge selection, similar to rapid STP
D. MSTP uses timers for transitioning the ports, similar to regular STP.

Correct Answer: B, C
Section:

QUESTION 24
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+.

Correct Answer: A, B
Section:

QUESTION 25
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

Correct Answer: B
Section:

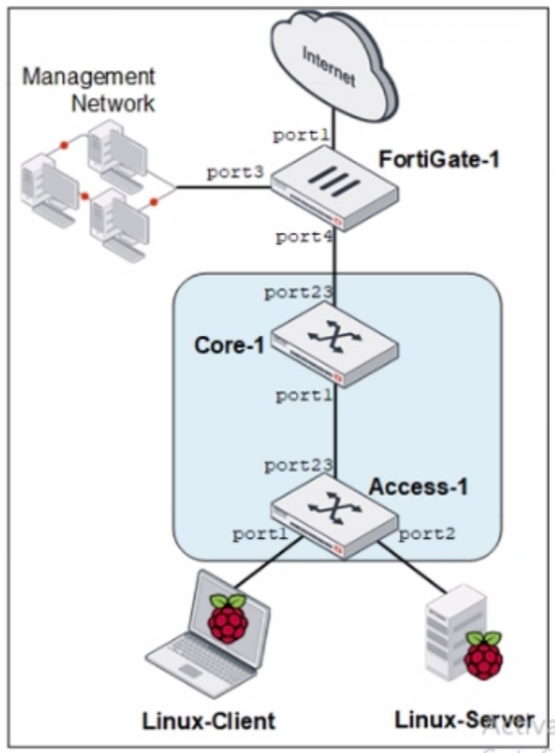
QUESTION 26
Which statement about 802.1X security profiles using MAC-based authentication mode is true?

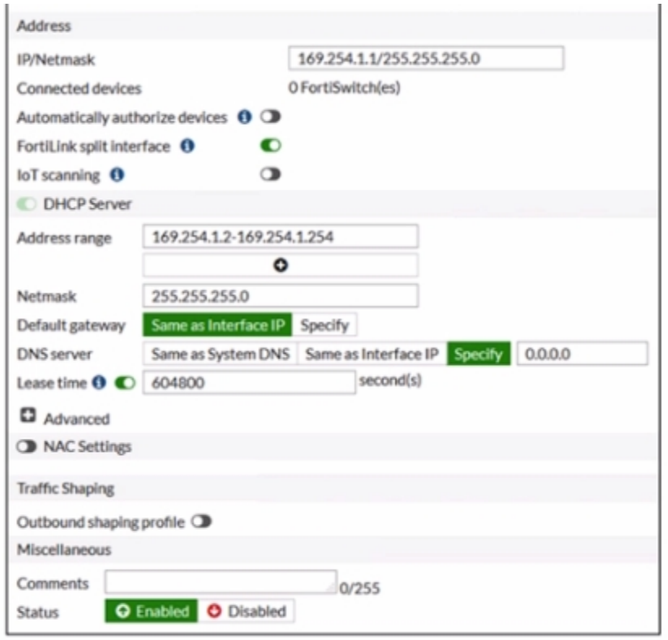
A. FortiSwitch allows connectivity to all hosts connected to a port, if one host is authenticated.
B. FortiSwitch can grant each device a different access level based on the credentials provided
C. FortiSwitch performs faster when using this security mode on the ports.
D. FortiSwitch must communicate with the RADIUS server to authenticate devices

Correct Answer: B
Section:

QUESTION 27
Refer to the exhibits.

Topology





You are asked to ensure that managed FortiSwitch devices are reachable by other devices, such as SNMP and other management tools across your network.
Which setting must you configure to ensure traffic from other devices in the network reaches FortiSwitch?

A. Select a specific default gateway provided to FortiSwitch as an upstream device.
B. Change the FortiLink interface IP address and DHCP server address range.
C. Recreate the FortiLink interface with a nonaggregate setting.
D. Enable NAC settings to select the onboarding VLAN.

Correct Answer: B
Section:

QUESTION 28
Which drop policy mode, if assigned to a congested port, will drop incoming packets until there is no congestion on the egress port?

A. Tail-drop mode
B. Weighted round robin mode.
C. Random early detection mode
D. Strict mode

Correct Answer: A
Section:

QUESTION 29
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.

Correct Answer: D
Section:

QUESTION 30
An administrator needs to deploy managed FortiSwitch devices in a remote location where multiple VLANs must be utilized to segment devices. No Layer 3 switch or router is present. The the only WAN connectivity is the router provided by the ISP connected to the public internet.
Which two items will the administrator need to use? (Choose two.)

A. A FortiSwitch interface connected to the ISP router configured with fortilink-13-mode enabled.
B. FortiSwitch and FortiGate devices configured with VXLAN interfaces.
C. FortiSwitch devices configured with NAT disabled.
D. FortiSwitch devices that have the required internal hardware for this configuration.
E. FortiSwitch and FortiGate devices configured with IPsec interfaces.

Correct Answer: B, C
Section:

QUESTION 31
What type of multimode transceiver can be used to split a 40G port?

A. QSFP+ transceiver
B. SFP transceiver
C. QSFP transceiver
D. SFP+ transceiver

Correct Answer: A
Section:

QUESTION 32
Which two statements about 802.1X authentication on FortiSwitch ports are true? (Choose two.)

A. All hosts behind an authenticated port are allowed access after a successful authentica-tion.
B. A security policy is used to apply 802.1 authentication on a port.
C. A local user database must be used to authenticate devices using the 802.1X authentica-tion protocol.
D. All devices connecting to FortiSwitch must support 802.1X authentication.

Correct Answer: A, B
Section:

QUESTION 33
Which two statements about managing a FortiSwitch stack on FortiGate are true? (Choose two.)

A. A FortiLink interface must be enabled on FortiGate.
B. The switch controller feature must be enabled on FortiGate.
C. Only a hardware-based FortiGate can manage a FortiSwitch stack.

D. FortiSwitch must be operating in standalone mode before authorization.

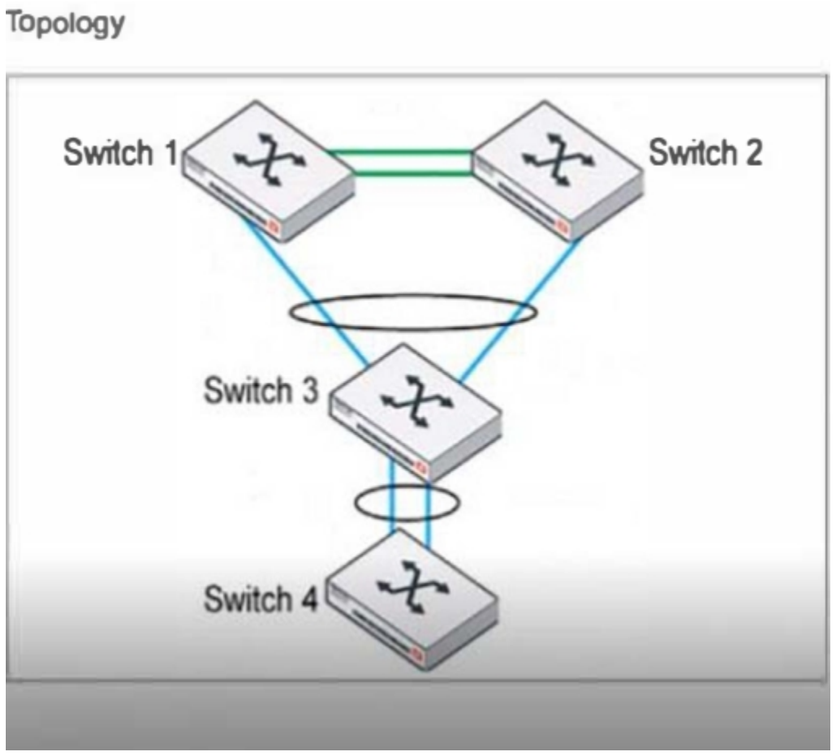
Correct Answer: A, B
Section:

QUESTION 34
How is traffic routed on FortiSwitch?

A. Hardware-based routing on FortiSwitch is handled by the CPU.
B. FortiSwitch looks up the hardware routing table and then the forwarding information base (FIB).
C. ASIC hardware routing can only handle dynamic routing, if supported.
D. Layer 3 routing can be configured on FortiSwitch, while managed by FortiGate.

Correct Answer: B
Section:

QUESTION 35
Exhibit.



LAG and MCLAG are used to increase the available network bandwidth and enable redundancy. How does spanning tree protocol see MCLAG and LAG if they are configured based on the physi-cal view shown in the exhibit? (Choose two)

A. Switch 1. Switch 2, and Switch 3 are seen as one MCLAG peer group
B. Switch 3 and Switch 4 uplinks are treated as single interfaces.
C. Switch 3 and switch 4 are seen as one MCLAG switch client
D. Switch 1 and Switch 2 both seen as one single switch.

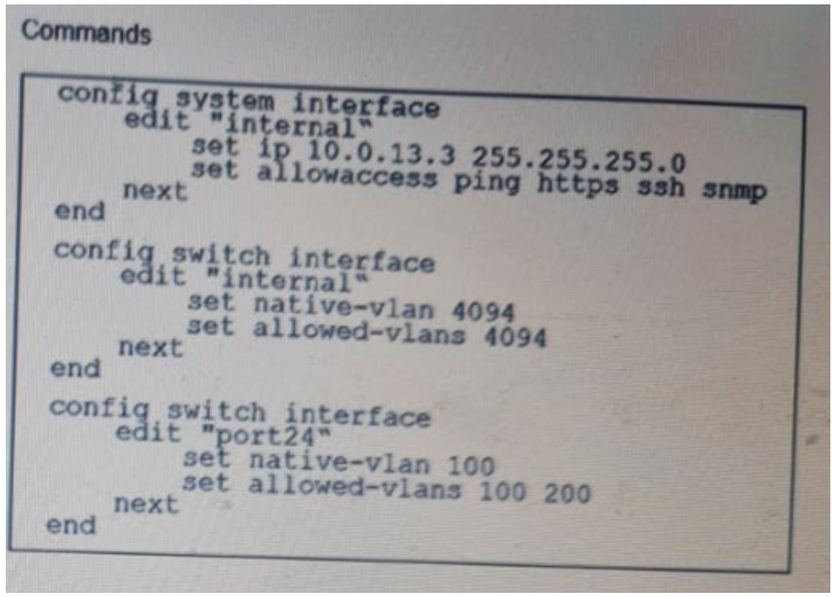
Correct Answer: C, D
Section:

QUESTION 36
Which statement about the configuration of VLANs on a managed FortiSwitch port is true?

A. Untagged VLANs must be part of the allowed VLANs: ingress and egress.
B. FortiSwitch VLAN interfaces are created only when FortiSwitch is managed by Forti-Gate.
C. The native VLAN is implicitly part of the allowed VLAN on the port.
D. Allowed VLANS expand the collision domain to the port.

Correct Answer: C
Section:

QUESTION 37
Exhibit.



port24 is the only uplink port connected to the network where access to FortiSwitch management services is possible. However, FortiSwitch is still not accessible on the management interface. Which two actions should you take to fix the issue and access FortiSwitch? (Choose two.)

A. You must add port24 native VLAN as an allowed VLAN on internal.
B. You must add VLAN ID 200 to the allowed VLANS on internal.
C. You must allow VLAN ID 4094 on port24, if management traffic is tagged.
D. You should use VLAN ID 4094 as the native VLAN on port24.

Correct Answer: C, D
Section:

QUESTION 38
How are the 'by VLAN redirect MAC address quarantine' mode and the 'by redirect MAC address quarantine' mode on FortiGate similar?

A. Both modes move quarantined devices to the quarantine VLAN.
B. Both modes require firewall policies to block inter-VLAN traffic.
C. Both modes add quarantined device MAC addresses to the blocked firewall address group.
D. Both modes block intra-VLAN traffic by FortiGate automatically.

Correct Answer: D
Section: