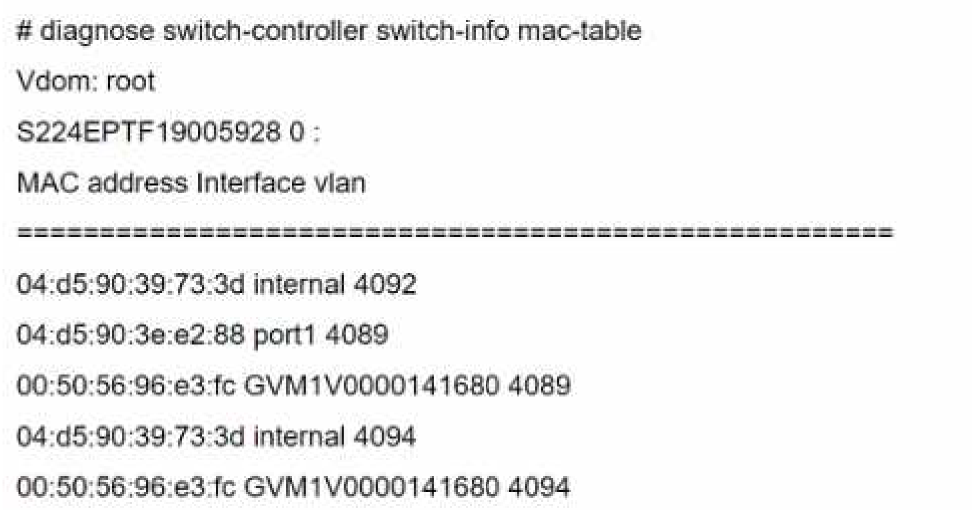
Latest Version: 7.1

Question: 1

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.

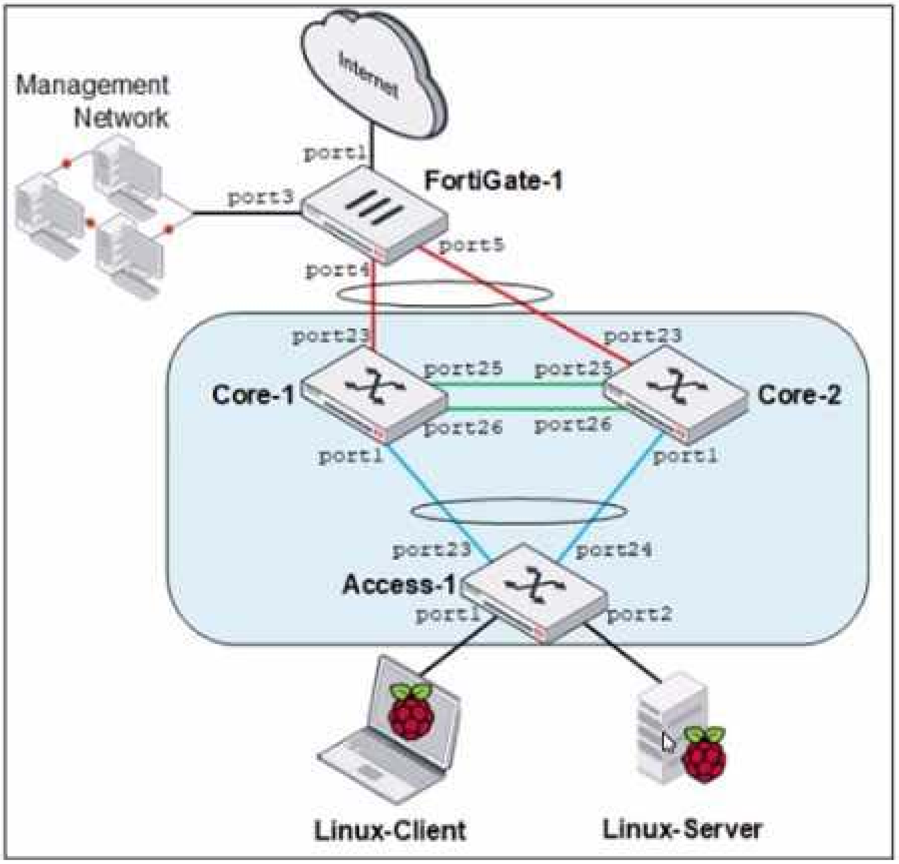
Answer: B

Explanation:
The MAC address "00:50:56:96:e3:fc" appearing in two different VLANs (4089 and 4094) in the diagnostic output indicates it is a MAC address associated with a device that supports traffic from multiple VLANs.
Such a behavior is typical of network infrastructure devices like switches or routers, which are configured to allow traffic from various VLANs to pass through a single physical or logical interface. This is essential in network designs that utilize VLANs to segregate network traffic for different departments or use cases while using the same physical infrastructure.
Reference:
For more detailed information on MAC table diagnostics and VLAN configurations in FortiGate devices, refer to the official Fortinet documentation: Fortinet Product Documentation.

Question: 2

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.

Answer: B

Explanation:
The STP (Spanning Tree Protocol) discarding state on port1 of Core-2, after Core-1 and Access-1 are managed and authorized by FortiGate-1, is likely due to the lack of an MCLAG (Multi-Chassis Link Aggregation Group) configuration between Core-1 and Core-2. In typical network configurations involving STP and MCLAG, the absence of MCLAG can lead to STP blocking one of the redundant paths to prevent loops, which is a critical function of STP. Port1 on Core-2 being in a discarding state suggests that it has been identified as providing a redundant path that could potentially create a network loop, hence STP has placed this port in a blocking (discarding) state to maintain a loop-free topology.
Reference:

For a deeper understanding of STP operations and MCLAG configurations in FortiGate managed environments, consult the Fortinet knowledge base: Fortinet Knowledge Base.

Question: 3

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.

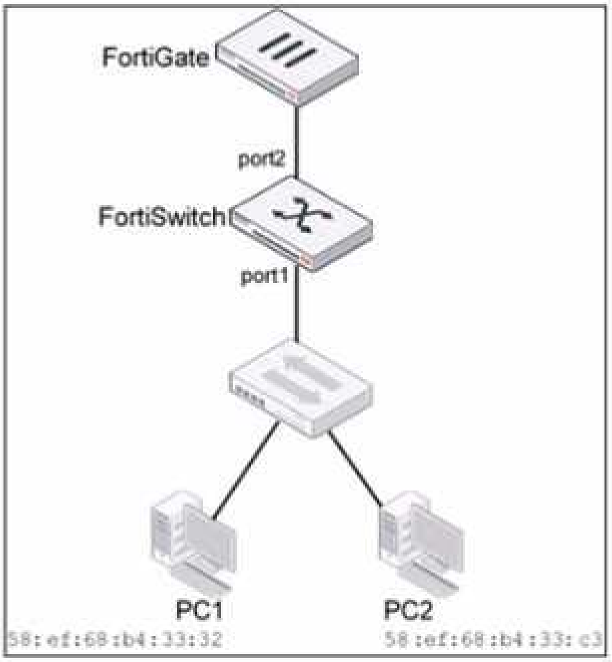
Answer: C, D

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 frame initiates 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.
Reference:
Further details on the FortiLink setup and authorization process can be accessed through the FortiGate configuration guides available on the Fortinet Documentation site.

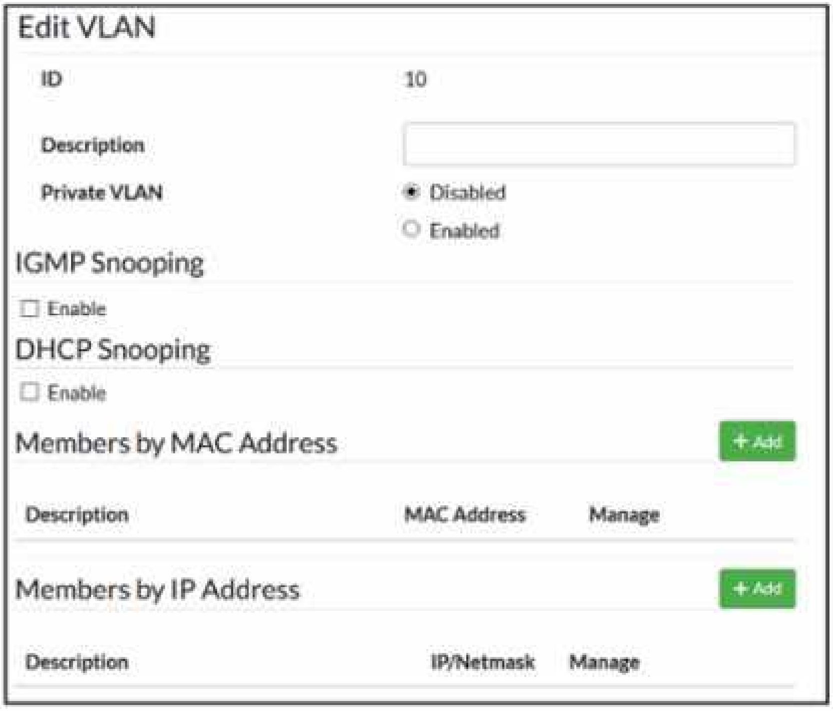
Question: 4

Refer to the exhibits

Topology



VLAN



Edit VLAN

ID	10
Description	
Private VLAN	● Disabled ○ Enabled

IGMP Snooping

□ Enable

DHCP Snooping

□ Enable

Members by MAC Address + Add

Description	MAC Address	Manage

Members by IP Address + Add

Description	IP/Netmask	Manage

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.

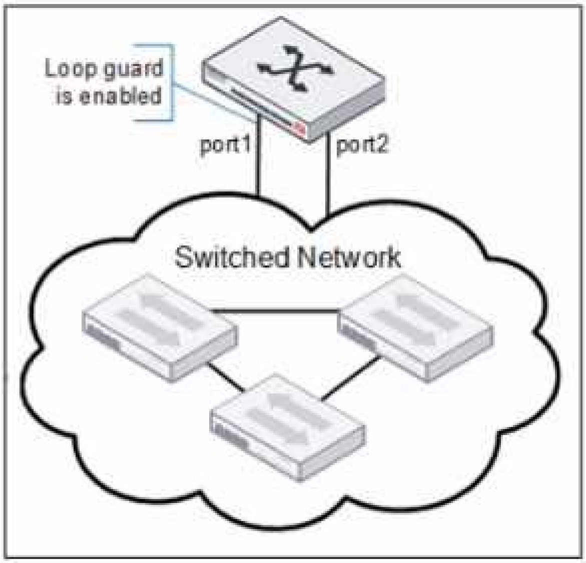
Answer: AB

Explanation:
The two reasons why port1 can be shut down are loop guard protection and Spanning Tree Protocol (STP).
Loop guard protection: This is a feature that helps to prevent switching loops in a network.expand_more A loop guard can be configured on a port to monitor for specific traffic patterns that indicate a loop. If loop guard protection detects a loop, it will shut down the port to prevent the loop from causing problems.
STP: STP is a protocol that helps to prevent switching loops.expand_more When multiple paths exist between two network devices, STP will block all but one of the paths, creating a loop-free topology.expand_more If STP detects a loop, it will shut down the ports that are involved in the loop.
In the exhibit, both ports 1 and 2 are configured with the same native VLAN 10. This configuration could create a switching loop if both ports are connected to devices on the same network segment. If a loop occurs, loop guard protection or STP could shut down port1 to prevent the loop from causing problems.
Reference:
Fortinet FortiSwitch 7.2 Administration Guide
https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/954635/getting-started

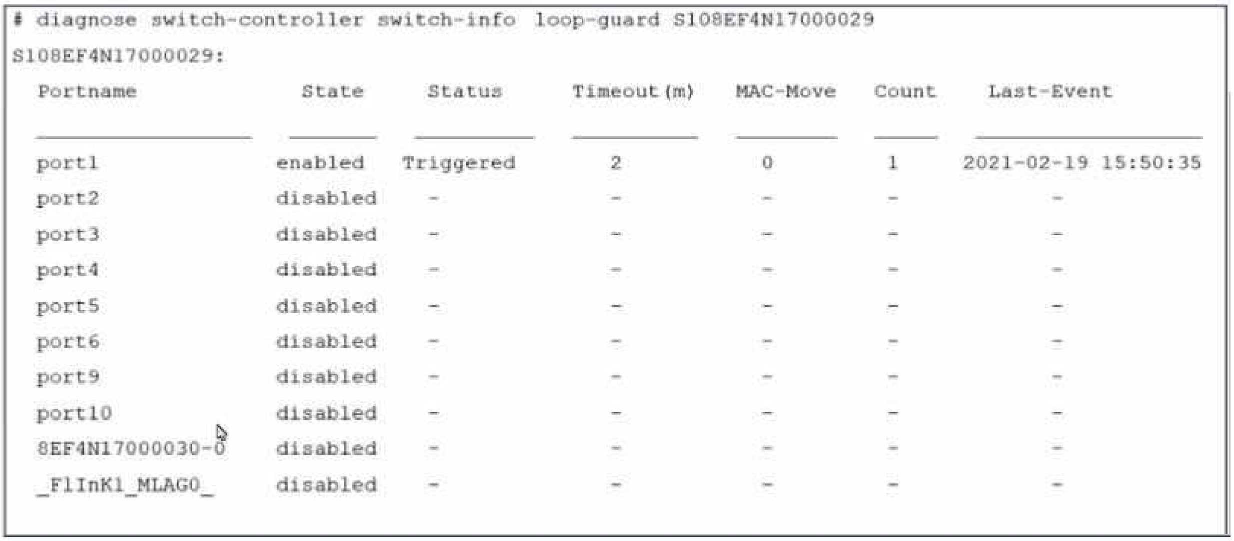
Question: 5

Refer to the exhibits.

LoopGuard-setup



LoopGuard-setup [redacted]



```
# 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.

Answer: AB

Explanation:
When loop guard is enabled on port1 and port2 configured with the same native VLAN (VLAN 10), there

are specific scenarios under which port1 can be shut down due to loop guard operation:
A . port1 was shut down by loop guard protection. Loop guard is a specific feature used in network environments to prevent alternative or redundant loops. When loop guard is active, it can shut down a port if it stops receiving BPDU (Bridge Protocol Data Units) on a port that is expected to receive them, assuming a loop or link failure and putting the port into an inconsistent state to prevent potential loops.
B . STP triggered a loop and applied loop guard protection on port1. If the Spanning Tree Protocol (STP) detects a loop or loss of BPDU transmissions while loop guard is enabled, it will proactively shut down the port to prevent network instability or a broadcast storm. This is an essential function of loop guard within the context of STP, providing additional protection against topology changes that could introduce loops.
Reference:
Additional details about loop guard functionality and STP interaction can be found in the FortiSwitch administration guides, accessible via Fortinet Documentation.