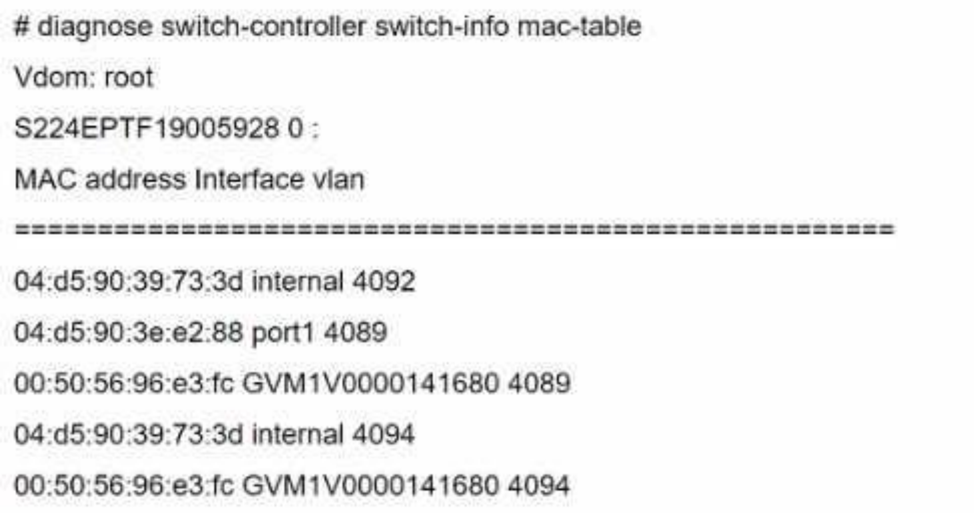
Vendor: Fortinet

Exam Code: NSE6_FSW-7.2

Exam Name: Fortinet NSE 6 - FortiSwitch 7.2

Version: DEMO

QUESTION 1
Refer to the diagnostic output:



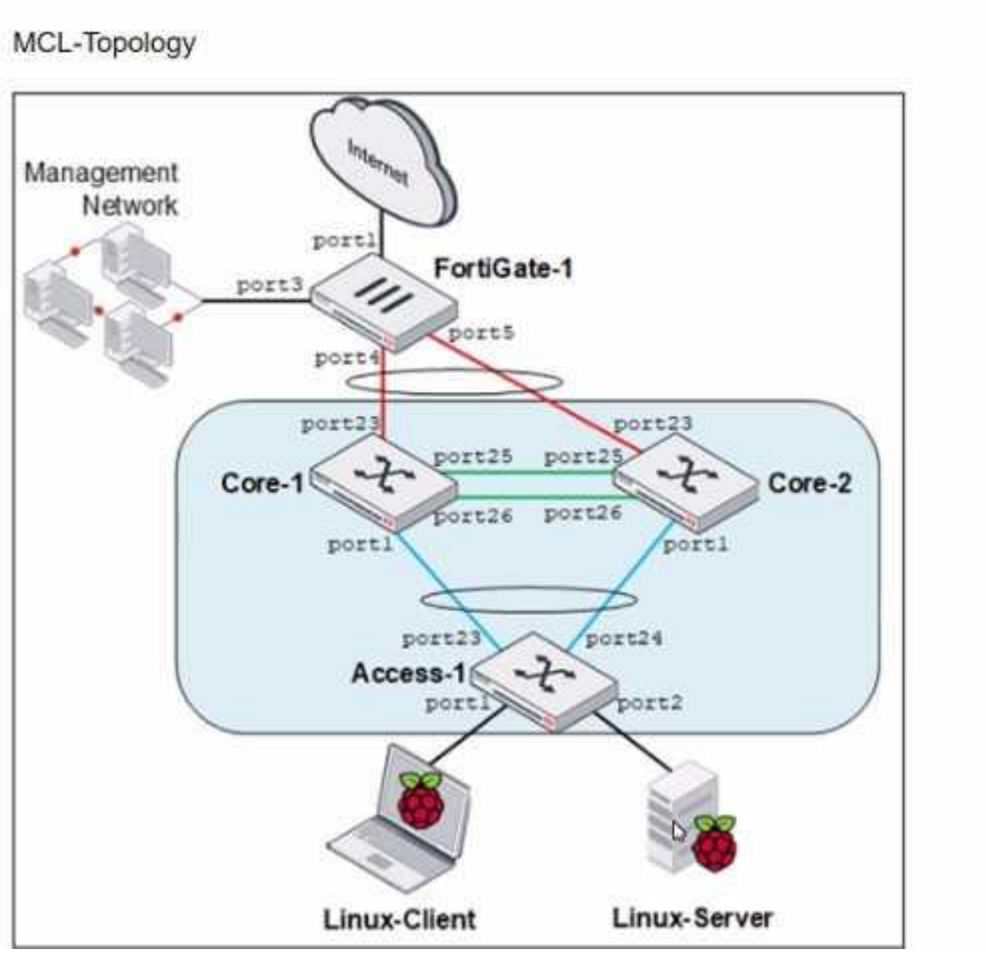
```
# diagnose switch-controller switch-info mac-table
Vdom: root
S224EPTF19005928 0 :
MAC address Interface vlan
=======================================================
04:d5:90:39:73:3d internal 4092
04:d5:90:3e:e2:88 port1 4089
00:50:56:96:e3:fc GVM1V0000141680 4089
04:d5:90:39:73:3d internal 4094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

QUESTION 2
Refer to the exhibit.



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

QUESTION 3
Which two statements about the FortiLink authorization process are true? (Choose two.)

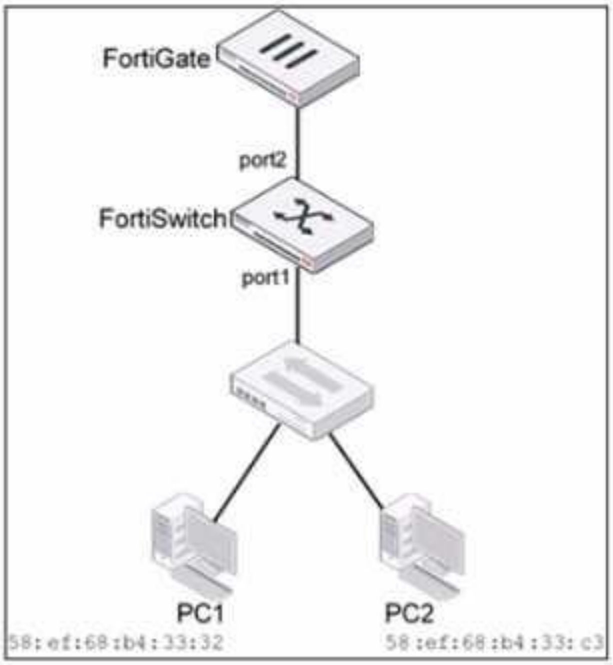
A. The administrator must manually pre-authorize FortiGate on FortiSwitch by adding the FortiGate serial number.
B. FortiSwitch requires a reboot to complete the authorization process.
C. A FortiLink frame is sent by FortiGate to FortiSwitch to complete the authorization.
D. FortiLink authorization sets the FortiSwitch management mode to FortiLink.

Answer: CD

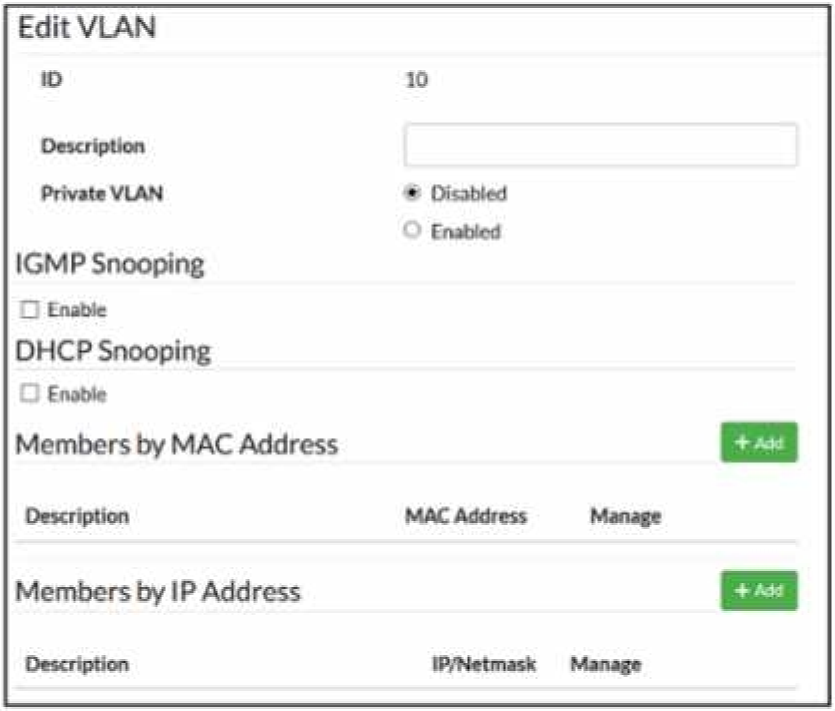
QUESTION 4

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

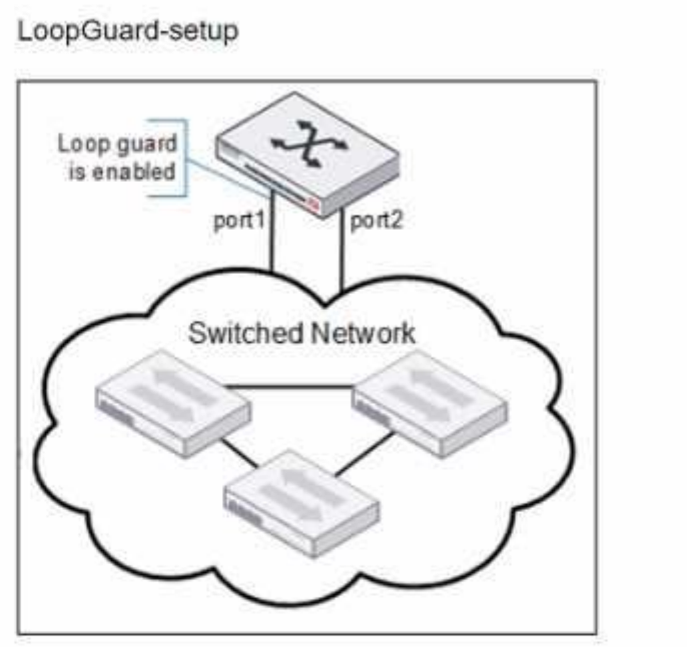
Description	IP/Netmask	Manage

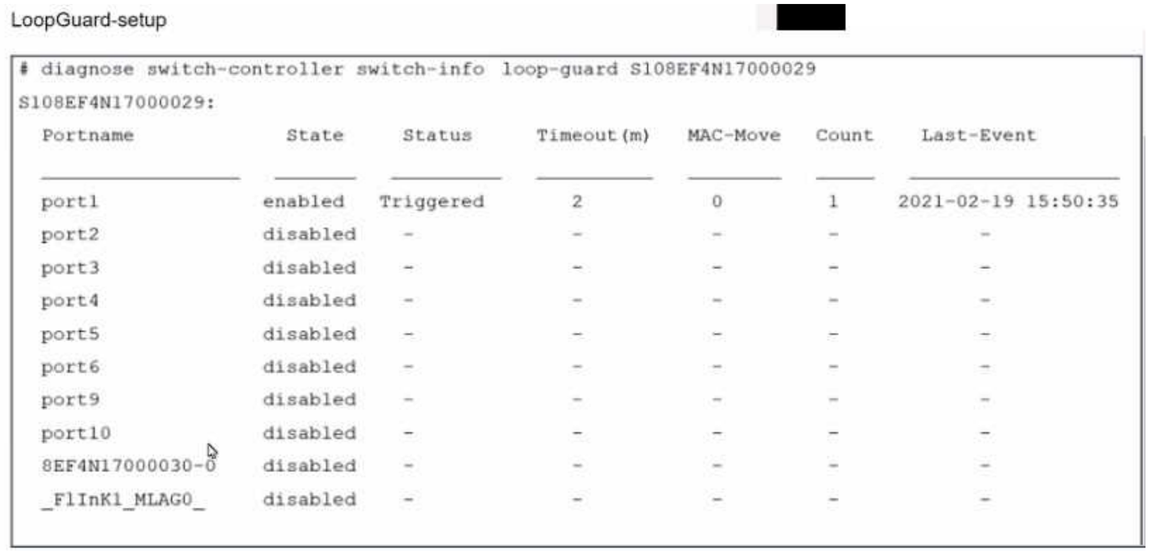
Traffic arriving on port2 on FortiSwitch is tagged with VLAN ID 10 and destined for PC1 connected on port1. PC1 expects to receive traffic untagged from port1 on FortiSwitch. Which two configurations can you perform on FortiSwitch to ensure PC1 receives untagged traffic on port1? (Choose two.)

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

QUESTION 5
Refer to the exhibits.





LoopGuard-setup [redacted]

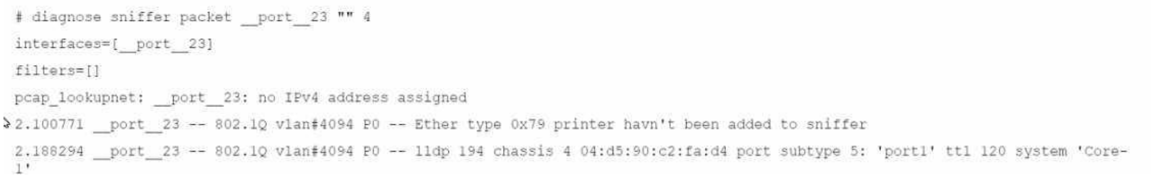
```
# diagnose switch-controller switch-info  loop-guard S108EF4N17000029
S108EF4N17000029:
   Portname                 State     Status      Timeout(m)    MAC-Move   Count     Last-Event
   ____________________   ________  __________   ___________   _________  ______  ____________________
   port1                  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: BC

QUESTION 6
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

Answer: A