PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 5FortiSwitch 7.6 Administrator

Fortinet NSE5_FSW_AD-7.6

Version Demo

Total Demo Questions: 9

Total Premium Questions: 90

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSwitch Overview	3
Topic 2, FortiSwitch Management	16
Topic 3, FortiSwitch Configuration	16
Topic 4, VLANs	8
Topic 5, Spanning Tree Protocol	12
Topic 6, Link Aggregation	3
Topic 7, Multicast	1
Topic 8, Security	15
Topic 9, Quality of Service	2
Topic 10, Monitoring and Troubleshooting	14
Total	90

QUESTION NO: 1

Refer to the diagnostic output:

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

Explanation:

The types of packets captured is limited. The FortiSwitch CLI sniffer is a diagnostic aid, but it is not equivalent to a full packet capture performed through a dedicated packet-capture mechanism or a traffic mirror sent to an analyzer. Fortinet documentation notes that, although the sniffer command can capture traffic on switch ports, the packet types available through this command are very limited. Consequently, its output cannot be assumed to represent every frame or protocol traversing port 23. This limitation is inherent to the command's capture capability rather than being dependent on whether the port carries tagged traffic, belongs to a trunk, or is observed in a particular traffic direction. When troubleshooting requires a complete and reliable view of traffic, use supported monitoring approaches such as port mirroring and capture the mirrored traffic with an appropriate analyzer. The FortiSwitch administration documentation provides the relevant operational and troubleshooting context for switch diagnostics: FortiSwitch 7.6 Administration Guide. Fortinet's product documentation portal also provides version-specific CLI and administration references: FortiSwitch documentation.

QUESTION NO: 2

Exhibit.

You need to manage three FortiSwitch devices using a FortiGate device. Two of the FortiSwitch devices initiated a reboot after the authorization process. However, the FortiSwitch device with the configuration shown in the exhibit. did not reboot All three devices completed FortiLink manage-ment authorization successfully.

Why did the FortiSwitch device shown in the exhibit not reboot to complete the authorization pro-cess?

The management mode was set to use FortiLink mode.

A. Switch auto-discovery is enabled.

B. The management mode was set to use FortiLink mode.

C. The FortiSwitch device is scheduled to reboot as part the authorization process

D. The system time is not in-sync and is using a non-default value

ANSWER: B

Explanation:

The management mode was set to use FortiLink mode. A FortiSwitch must operate in FortiLink management mode to be centrally managed by a FortiGate through FortiLink. During authorization, FortiGate applies the managed-switch configuration and, where necessary, the FortiSwitch changes its management mode to FortiLink. A reboot is required when that management-mode transition must be applied. In this case, the displayed FortiSwitch was already configured for FortiLink management, so authorization could complete without an additional reboot. This behavior is expected: the reboot is associated with applying a required operating-mode change, rather than being an unconditional step for every successfully authorized FortiSwitch. Once authorized, the FortiGate can manage the switch and deploy the relevant FortiLink-controlled configuration while preserving the existing FortiLink operating mode. Fortinet documents FortiLink as the mechanism for FortiGate-managed FortiSwitch deployment and describes management-mode configuration in the FortiSwitch administration documentation. See the FortiGate FortiLink documentation and the FortiSwitch 7.6 Administration Guide.

QUESTION NO: 3

Which two types of Layer 3 interfaces can participate in dynamic routing on FortiSwitch? (Choose two.)

A. Detected management interfaces

B. Loopback interfaces

C. Switch virtual interfaces

D. Physical interfaces

ANSWER: B C

Explanation:

Loopback interfaces and **Switch virtual interfaces** can participate in FortiSwitch dynamic routing. A loopback interface is a logical Layer 3 interface that remains operational independently of an individual physical link. This makes it useful for a consistent routed address, including use as a stable router identifier or as a reliably reachable address advertised by a routing protocol. Because it is a Layer 3 logical interface, it can be included in the dynamic-routing configuration.

A switch virtual interface (SVI) is the Layer 3 interface associated with a VLAN. After an IP address is assigned, the SVI provides the routed gateway for devices in that VLAN and is an appropriate interface on which to run or advertise dynamic-routing information. This allows the VLAN subnet to be exchanged through supported routing protocols and enables routed connectivity between VLAN-based networks. FortiSwitch documentation describes dynamic-routing support and the Layer 3 interface model in the FortiSwitchOS Administration Guide. See the FortiSwitchOS 7.6 Administration Guide and the FortiSwitch 7.6 documentation portal for the relevant routing and interface configuration details.

QUESTION NO: 4

A FortiSwitch LACP aggregate is connected to an upstream switch. Both ends of the aggregate are configured in passive LACP mode, and none of the member links joins the aggregate.

Which change is required to establish the LACP aggregate? (Choose one answer)

A. Change one side of the aggregate from passive mode to active mode.

B. Configure both sides of the aggregate in passive mode and reboot the switches.

C. Configure a different native VLAN on each aggregate member.

D. Disable STP on every aggregate member interface.

ANSWER: A

Explanation:

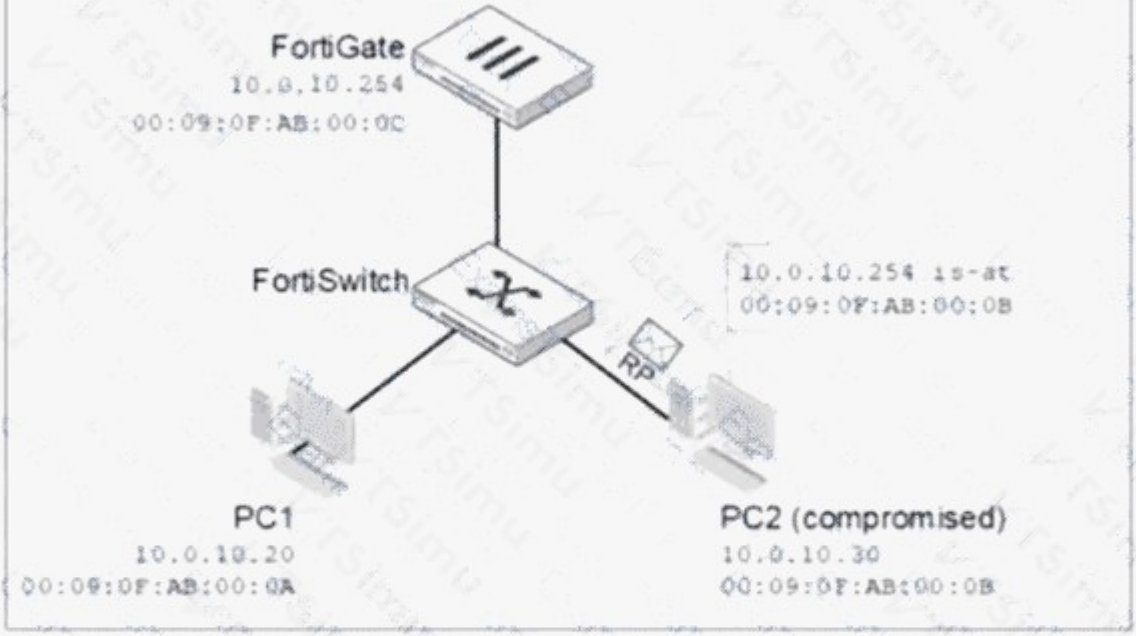
At least one side of an LACP connection must operate in active mode. An active LACP interface transmits LACP packets to initiate negotiation, whereas a passive interface waits to receive LACP packets before responding. When both ends are passive, neither device initiates the exchange, so the physical links do not become active aggregate members.

Changing either the FortiSwitch aggregate or the upstream aggregate to active mode allows LACP negotiation to begin. Static aggregation is not required and would remove the protocol-based validation provided by LACP.

QUESTION NO: 5

Refer to the exhibits.

Network Topology



DHCP Snooping database

DHCP Snooping Client DB

MAC	VLAN	IP	Interface
00:09:0F:AB:00:0A	10	10.0.10.20	port1
00:09:0F:AB:00:0B	10	10.0.10.30	port2

All three FortiSwitch-connected ports are configured in VLAN 10. FortiGate acts as the Dynamic Host Configuration Protocol (DHCP) server and is connected to a DHCP snooping trusted trunk port. PC1 and PC2 are connected to ports configured as untrusted for Dynamic ARP Inspection (DAI), and no static bindings are configured in the IP source guard (IPSG) database. PC2 is compromised and attempts to spoof the FortiGate IP address by sending forged Address Resolution Protocol (ARP) replies with its own MAC address. What will FortiSwitch do with the ARP packets from PC2? (Choose one answer)

A. Forward the ARP replies because there are no IPSG bindings blocking them.

B. Accept the ARP replies because the VLAN has DAI enabled and FortiGate is a trusted DHCP server.

C. Forward the ARP replies to all VLAN 10 ports because DAI is only active on trusted ports.

D. Drop the ARP replies because they fail DAI validation against the DHCP snooping database.

ANSWER: D

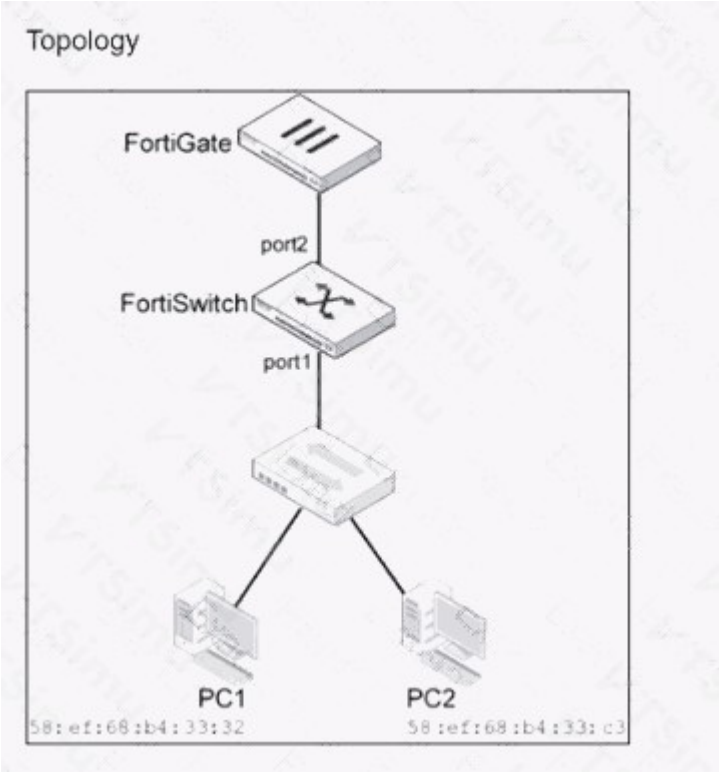
Explanation:

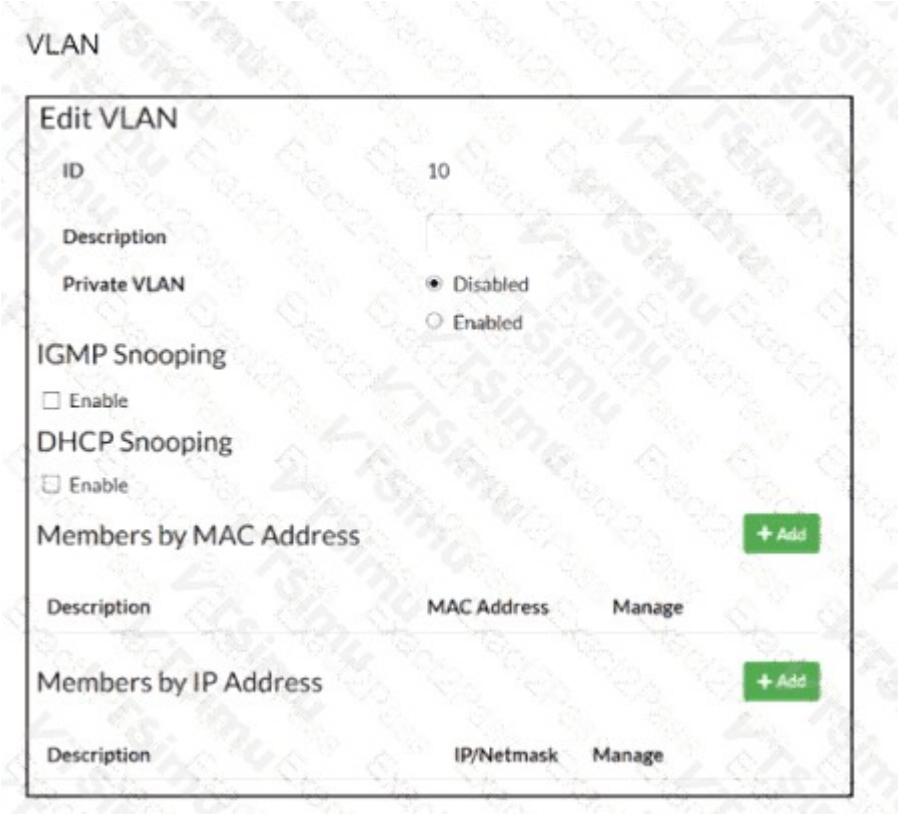
FortiSwitch will **drop the ARP replies because they fail DAI validation against the DHCP snooping database.** Dynamic ARP Inspection protects a VLAN against ARP spoofing by inspecting ARP traffic received on untrusted interfaces. For an ARP packet from an untrusted port to be permitted, its sender IP and sender MAC information must match a valid IP-to-MAC

binding learned through DHCP snooping, unless an applicable static DAI/IPSG binding is configured. In this topology, the trusted FortiGate-facing trunk permits DHCP snooping to learn the legitimate DHCP leases for the endpoints. Therefore, PC2 has a valid binding only for its assigned address and its own MAC address. Its forged ARP reply instead claims that the FortiGate's IP address belongs to PC2's MAC address. That IP-to-MAC pairing does not match the DHCP snooping binding table, so DAI identifies the ARP reply as invalid and discards it before it can poison ARP caches of hosts on VLAN 10. The lack of static IPSG entries does not prevent DAI from using DHCP snooping lease information for its validation. Fortinet documents DAI as a mechanism that validates ARP packets against DHCP snooping bindings to mitigate ARP spoofing and ARP cache-poisoning attacks. See the FortiSwitchOS 7.6 Administration Guide and FortiSwitchOS 7.6 documentation.

QUESTION NO: 6

Refer to the exhibits





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 PC1 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: B C

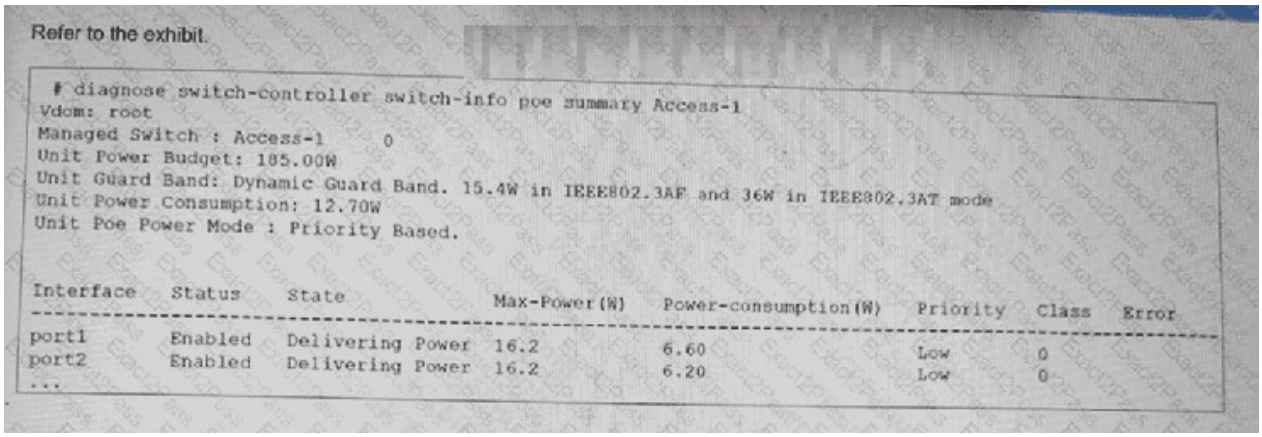
Explanation:

Adding VLAN ID 10 as a member of the untagged VLANs on port1 ensures that frames forwarded in VLAN 10 leave port1 without an IEEE 802.1Q VLAN header. The switch uses the VLAN membership and egress tagging configuration of the outgoing interface to decide whether to transmit a frame tagged or untagged. Because PC1 is connected to port1 and expects ordinary Ethernet frames, VLAN 10 must be configured as an untagged VLAN on that port.

Removing VLAN 10 from the allowed VLANs and adding it to untagged VLANs on port1 accomplishes the same required egress behavior through the interface VLAN-membership configuration workflow. It places VLAN 10 in the port's untagged membership rather than retaining it as a tagged/allowed VLAN for trunk-style forwarding. Consequently, traffic received on port2 with VLAN ID 10 can be switched to port1 and has its VLAN tag removed before delivery to PC1. This configuration maintains VLAN segmentation within the switch and presents PC1 with the untagged access-port behavior it requires. FortiSwitch VLAN and port VLAN-membership behavior is documented in the FortiSwitchOS 7.6 Administration Guide and the related FortiSwitch 7.6 documentation.

QUESTION NO: 7

Refer to the exhibit.



The FortiSwitch CLI output of the diagnose switch-controller switch-info poe summary command for the switch Access-1 is shown. It shows that two ports have Power over Ethernet (PoE) enabled and are already in use. What is the most important consideration if you want to connect additional PoE devices to FortiSwitch? (Choose one answer)

A. All plugged devices use the same PoE standard: 802.3af/at.

B. The FortiSwitch model supports the number of PoE devices that you want to connect.

C. The PoE power mode matches the PoE standard of the device.

D. The total PoE consumption must not exceed the FortiSwitch power budget.

ANSWER: D

Explanation:

The total PoE consumption must not exceed the FortiSwitch power budget. A FortiSwitch has a finite PoE power budget, representing the amount of power that its power supply can make available collectively to powered devices. Before attaching additional access points, IP phones, cameras, or other PoE-powered devices, the administrator must account for the current PoE consumption and the expected power requirements of the new devices. The combined allocation or consumption must remain within the available budget so that the switch can deliver stable power to all connected devices.

The displayed PoE summary provides the key values for this decision: unit power budget, current unit power consumption, and guard-band information. The guard band reserves capacity to accommodate power changes, particularly when devices start up or alter their power draw. Therefore, planning should use the available power after considering both the existing consumption and the applicable guard-band behavior. FortiSwitch also supports PoE power-management behavior such as priority-based allocation, which makes the configured budget and port priorities operationally significant when demand is high. Fortinet documents PoE configuration and monitoring in the FortiSwitchOS Administration Guide. General IEEE PoE power classifications and requirements are maintained by the IEEE 802.3af standard.

QUESTION NO: 8

You are troubleshooting a local port-mirroring session on a standalone FortiSwitch. A packet analyzer is connected to the mirror destination port, and the administrator must inspect both packets entering and leaving a server-facing source port.

Which two statements are true? (Choose two answers)

A. The source port can be configured to mirror both ingress and egress traffic.

B. The packet analyzer must be connected to the configured destination port.

C. The source port and destination port must use the same native VLAN.

D. Port mirroring changes the VLAN assignment of the original server traffic.

E. The destination port must be configured as a DHCP snooping trusted port.

ANSWER: A B

Explanation:

A local port-mirroring session can be configured to copy ingress traffic, egress traffic, or both directions from the selected source port. To inspect the complete conversation to and from the server, the source direction must include both ingress and egress traffic.

The destination port forwards the copied packets to the attached analyzer. It is not an ordinary user-facing port for normal production traffic while it is being used as a mirror destination.

QUESTION NO: 9

Refer to the exhibit.

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:

FortiSwitch is configured to trust DHCP replies coming on FortiLink interface. The DHCP snooping status identifies `FlInK1` among the trusted ports. A trusted DHCP snooping port is permitted to receive DHCP server messages, including offers and acknowledgments. This is the required configuration when the legitimate DHCP server, or an upstream device relaying DHCP server responses, is reached through the FortiLink connection. FortiSwitch uses this trust designation to distinguish valid server-side DHCP traffic from traffic arriving on untrusted access-facing ports.

Global configuration for DHCP snooping is set to forward DHCP client requests on all ports in the VLAN. The displayed DHCP broadcast mode of `All` means DHCP client broadcast requests are forwarded to all eligible ports in the VLAN, rather than being restricted to only trusted ports. This allows client DHCP Discover and Request broadcasts received on access ports to reach the legitimate DHCP service path while DHCP snooping continues to apply its inspection and trust policy to DHCP server responses. Fortinet documents DHCP snooping trusted-port behavior and DHCP broadcast forwarding modes in the FortiSwitch Administration Guide: DHCP snooping and the associated FortiSwitch CLI Reference.