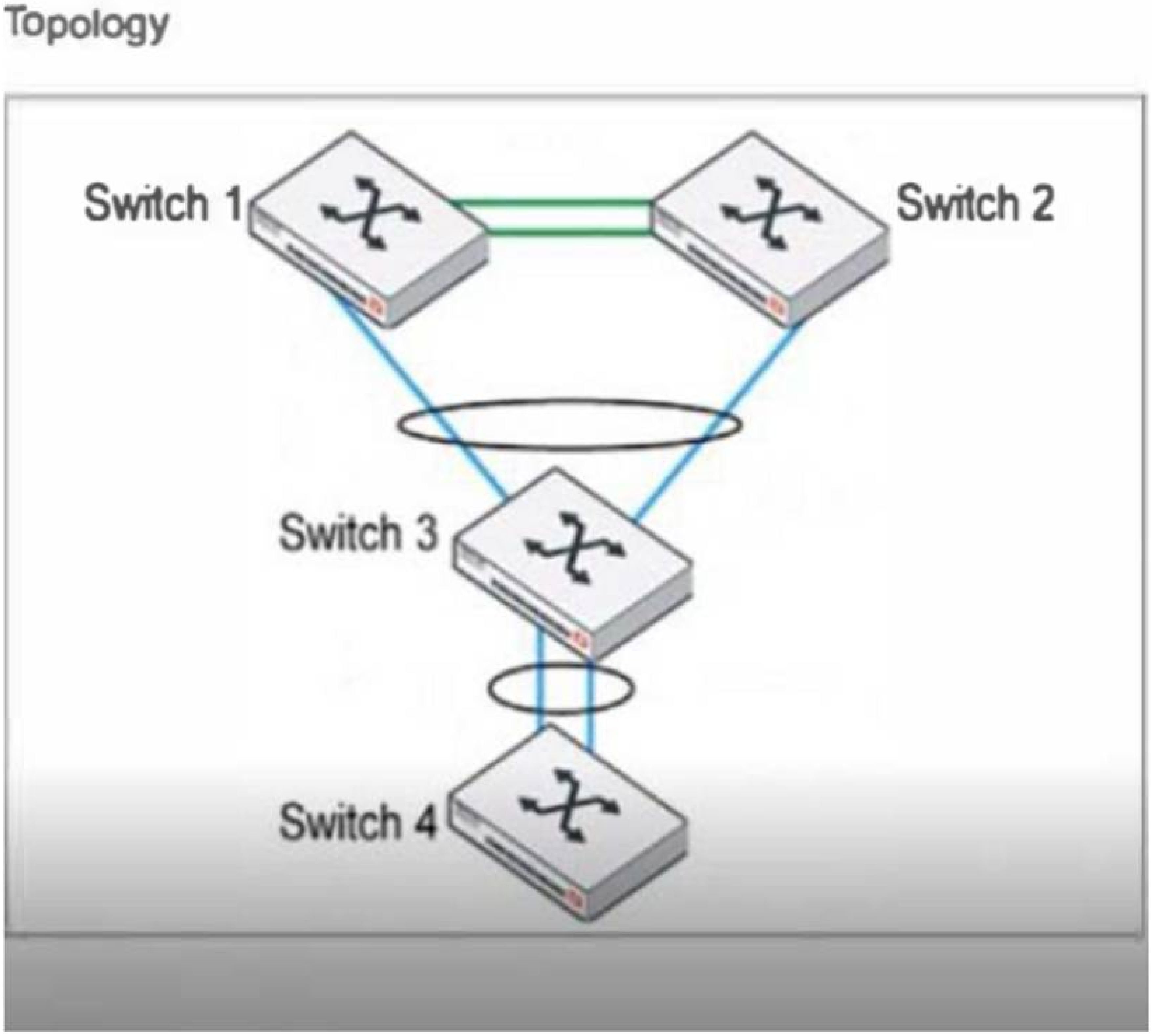
Fortinet

Exam Questions NSE6_FSW-7.2

Fortinet NSE 6 - FortiSwitch 7.2

NEW QUESTION 1
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.

Answer: AB

Explanation:
In the context of the topology provided and the concepts of LAG (Link Aggregation Group) and MCLAG (Multi-Chassis Link Aggregation), the spanning tree protocol's perspective can be summarized as follows:

➢ Switch 1, Switch 2, and Switch 3 are seen as one MCLAG peer group (Option A): In this configuration, Switches 1 and 2 form a Multi-Chassis Link Aggregation Group (MCLAG) which effectively allows them to act as a single logical entity from the perspective of downstream switches (in this case, Switch 3). This grouping enhances fault tolerance and bandwidth by pooling the link resources of the two switches.

➢ Switch 3 and Switch 4 uplinks are treated as single interfaces (Option B): This option suggests that the connections between Switch 3 and Switch 4 (presumably using LAG) are perceived by the spanning tree protocol as a single logical connection. This perception is due to the LAG configuration, which combines multiple network cables/ports into a single logical link to provide redundancy and increase bandwidth.
References:

➢ The use of LAG and MCLAG is well-documented in networking literature and Fortinet's own documentation, as these technologies are commonly employed to enhance redundancy and bandwidth. Fortinet's implementation of these protocols is designed to maintain compatibility with standard networking protocols, including Spanning Tree Protocol (STP).

NEW QUESTION 2
In which two ways can you assign a FortiSwitch port to a VDOM using multi-tenancy setup? (Choose two.)

A. Switch the FortiLink interface to the target VDOM.
B. Remove the managed FortiSwitch and allocate ports directly on FortiSwitch.

C. Create a virtual port pool on the FortiGate CLI.
D. Assign a port to a VDOM directly on the managed FortiSwitch.

Answer: AC

Explanation:
In a multi-tenancy setup on FortiGate, you can assign a FortiSwitch port to a VDOM in two primary ways:

➤ Switch the FortiLink Interface to the Target VDOM (A): This method involves configuring the FortiLink interface, which is the dedicated interface used to manage FortiSwitch units from FortiGate, to operate within a specific VDOM. This effectively assigns all ports on the FortiSwitch, managed through that FortiLink interface, to the designated VDOM.

➤ Create a Virtual Port Pool on the FortiGate CLI (C): Virtual port pools are created on FortiGate and allow ports from FortiSwitch to be grouped and assigned to a VDOM. This method is more granular and flexible, as it allows specific ports on the FortiSwitch to be dedicated to different VDOMs without requiring the entire switch or FortiLink interface to be dedicated to a single VDOM.

NEW QUESTION 3
To enhance service in emergency situations, to which LLDP-MED Type-Length-Values does Forti-Switch advertise to IP phones?

A. Network policy
B. Inventory management
C. Location
D. Power management

Answer: C

Explanation:
Location (C): FortiSwitch uses LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) to advertise various attributes to IP phones, among which "Location" is crucial in emergency situations. This information helps emergency responders to determine the physical location of the calling device, which is vital for prompt response in critical situations.

NEW QUESTION 4
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):
References:For a comprehensive guide on configuring ACLs in FortiSwitch, consult the FortiSwitch security settings documentation available on:Fortinet Product Documentation

NEW QUESTION 5
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

Answer: A

Explanation:
QSFP+ transceiver (A): The QSFP+ (Quad Small Form-factor Pluggable Plus) transceiver is designed to handle 40G data rates and can be used to split a 40G port into multiple 10G connections. This type of transceiver supports such configurations, making it suitable for high-density applications where multiple 10G connections are derived from a single 40G port, thereby maximizing the utilization of the port and the fiber infrastructure.

NEW 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.

Answer: AC

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.

NEW 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.

Answer: B

Explanation:
The correct statement about the quarantine VLAN on FortiSwitch is:
* B. Users who fail 802.1X authentication can be placed on the quarantine VLAN.This feature allows network administrators to isolate devices that do not meet the network??s security criteria as determined through 802.1X authentication. Placing these devices in a quarantine VLAN restricts their network access, thereby protecting the network from potential security threats posed by unauthorized or compromised devices.
Option A is incorrect as the presence of a DHCP server in a quarantine VLAN depends on specific network configurations. Option C is incorrect without more context regarding global settings, and option D misstates the functionality of quarantine VLANs, as their primary use is to restrict, not block, devices without additional VLAN configuration changes.

NEW QUESTION 8
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 theInventory ManagementTLV.
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.

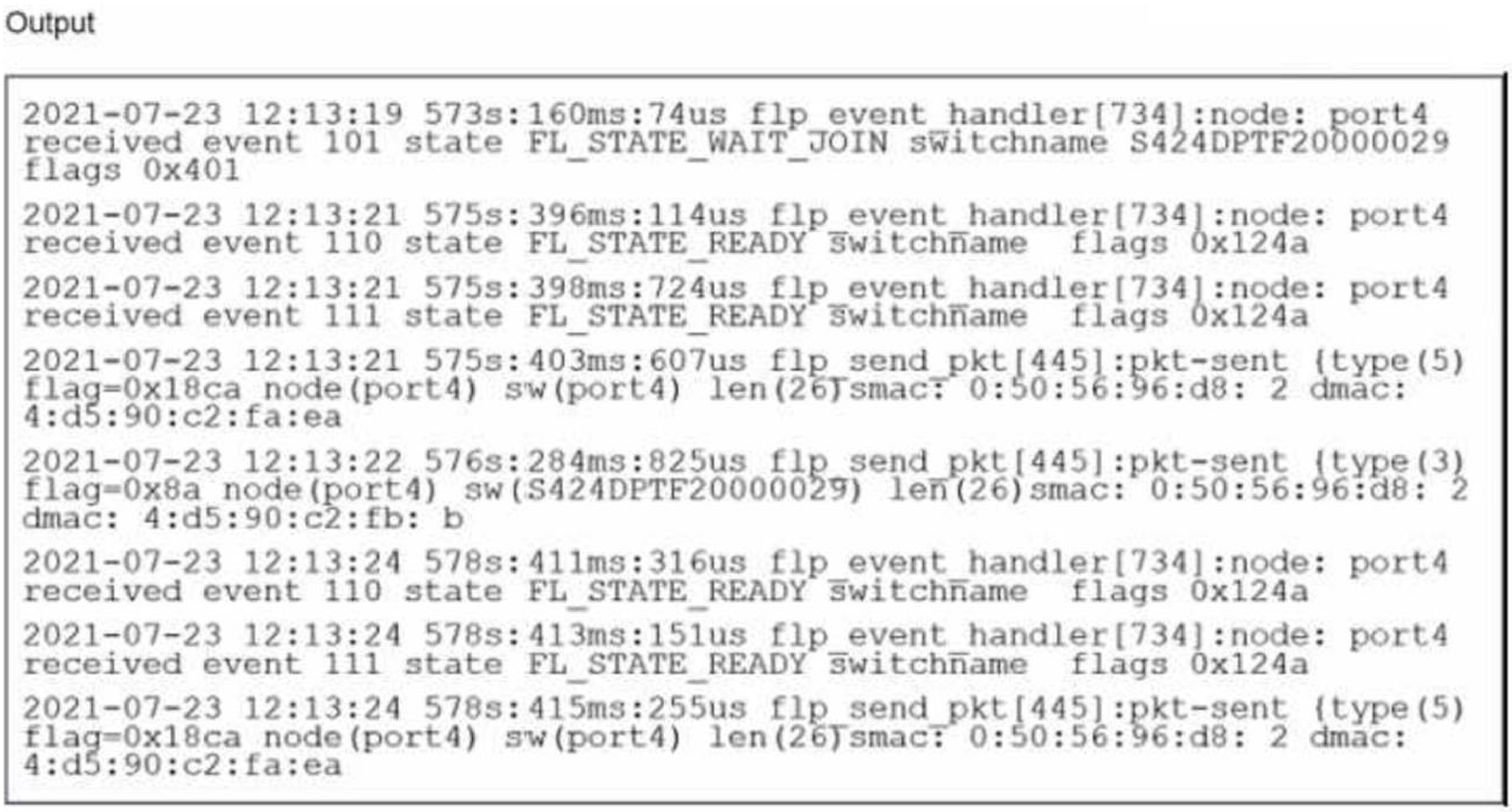
NEW QUESTION 9
Which statement about using MAC, IP, and protocol-based VLANs on FortiSwitch is true?

A. It is a scalable and secure solution in comparison to other Layer 2 security measures.
B. FortiSwitch uses only the Ethernet type to assign traffic to VLANs.
C. It provides benefits that can be obtained when using 802.1X authentication.
D. Endpoints are required to use the same FortiSwitch port to remain members of the VLAN.

Answer: C

Explanation:
It provides benefits that can be obtained when using 802.1X authentication (C): MAC, IP, and protocol-based VLANs on FortiSwitch are beneficial in network environments where additional granularity is needed in traffic segmentation and security, similar to what can be achieved through 802.1X authentication. These VLAN types allow for dynamic assignment of ports to VLANs based on the characteristics of the incoming traffic, enhancing both security and network efficiency.

NEW QUESTION 10
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
```

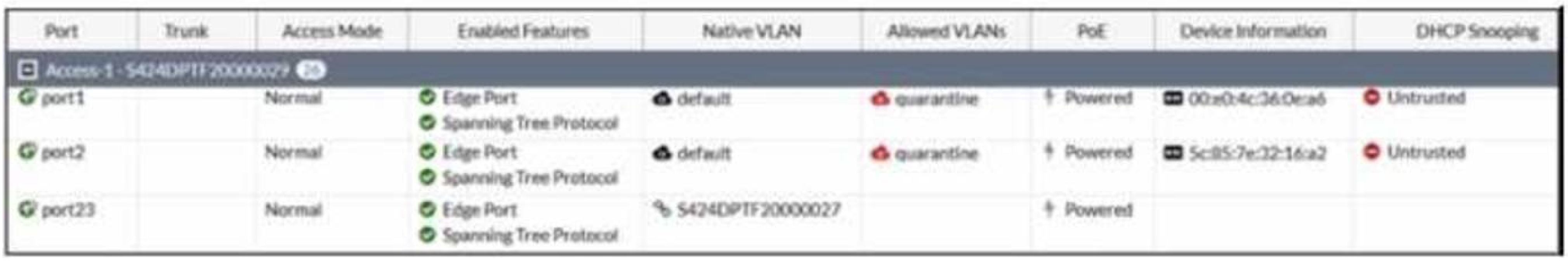
Which two statements best describe what is displayed in the FortiLink debug output shown in the exhibit? (Choose two.)

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.

Answer: AB

Explanation:
The provided debug output indicates that the FortiSwitch is sending FortiLink heartbeats to the FortiGate and is currently waiting to join the stack group. Here's a breakdown of the relevant lines:
Line 1:Shows the date, time, elapsed time since boot, and process ID for the FortiLink event handler.
Event 101:This indicates the FortiSwitch is in a "wait join" state (FL_STATE_WAIT_JOIN). This means it's discovered by the FortiGate and is awaiting further instructions to join the FortiLink stack group.
switchname S424DPTF20000029:This displays the serial number of the FortiSwitch.
flags 0x401:The specific flag meaning might depend on the FortiSwitch model and version, but it likely indicates general communication between the switch and FortiGate.
Lines 2 and onward:These lines show subsequent events with similar timestamps, suggesting a regular heartbeat interval. There are also instances of the FortiSwitch sending packets to the FortiGate (indicated bypkt-sent).
Why the Other Options Are Less Likely:
* C. FortiSwitch is discovered and authorized by FortiGate.While discovery might have happened before these lines, the "wait join" state suggests authorization hasn't necessarily completed yet.
* D. FortiSwitch is ready to push its new hostname to FortiGate.There's no explicit indication of hostname changes in this excerpt. The focus is on joining the stack group.
In Summary:
The key point is the "FL_STATE_WAIT_JOIN" state, which signifies the FortiSwitch is ready to be fully integrated but is waiting for further commands from the FortiGate to complete the process.

NEW QUESTION 10
Refer to the exhibit.



Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping
⊟ Access-1 - S424DPTF20000029 (26)								
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.

Answer: D

Explanation:
The information in the "Native VLAN" column for port23 on the FortiSwitch indicates that a standalone switch is connected to it. This is because the column displays "$424MPTF20000027," which matches the format of a Fortinet device serial number.
Here's a breakdown of the evidence in the image:
Native VLAN:The "Native VLAN" column typically displays the VLAN ID for untagged traffic on a trunk port. However, in this case, it shows a serial number format ("$424MPTF20000027").
No Trunk Information:The "Trunk" column is blank for port23, indicating it's not configured as a trunk member.
Other Ports:Port1 and port2 show "default" in the "Native VLAN" column, which is the expected behavior for access ports.
Fortinet FortiSwitch devices typically don't display the serial number of adjacent FortiSwitch devices in the "Native VLAN" column. This column is reserved for VLAN information on trunk ports.

NEW QUESTION 11
Which feature should you enable to reduce the number or unwanted IGMP reports processed by the IGMP querier?

A. Enable the IGMP flood setting on the static port for all multicast groups.
B. Enable the IGMP flood reports setting on the mRouter port.
C. Enable IGMP snooping proxy.
D. Enable IGMP flood unknown multicast traffic on the global setting.

Answer: C

Explanation:
Enable IGMP snooping proxy (C): To reduce the number of unwanted IGMP reports processed by the IGMP querier, enabling IGMP snooping proxy is effective. This feature acts as an intermediary between multicast routers and hosts, optimizing the management of IGMP messages by handling report messages locally and reducing unnecessary IGMP traffic across the network. This minimizes the processing load on the IGMP querier and improves overall network efficiency.

NEW QUESTION 16
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.

Answer: C

Explanation:
The issue described pertains to the establishment of a tunnel (likely a CAPWAP tunnel for management purposes between FortiGate and FortiSwitch). Based on typical error analysis in tunnel setup scenarios:
The CAPWAP tunnel failed to come up due to a mismatch in time (Option C): This answer is plausible because time synchronization is crucial for security protocols that underpin tunnel establishments, such as DTLS (Datagram Transport Layer Security) used within CAPWAP tunnels. If the clocks on FortiGate and FortiSwitch are significantly out of sync, the security handshake (which can include timestamp validation) could fail, preventing the tunnel from coming up.
References:
Fortinet's technical documentation typically outlines the importance of time synchronization for secure communications. In CAPWAP/DLTS scenarios, precise time matching is crucial to ensure that the cryptographic parameters align correctly during the handshake process.

NEW QUESTION 18
......