# Free Questions for NSE6_FSW-7.2

## Shared by Vaughn on 03-03-2025

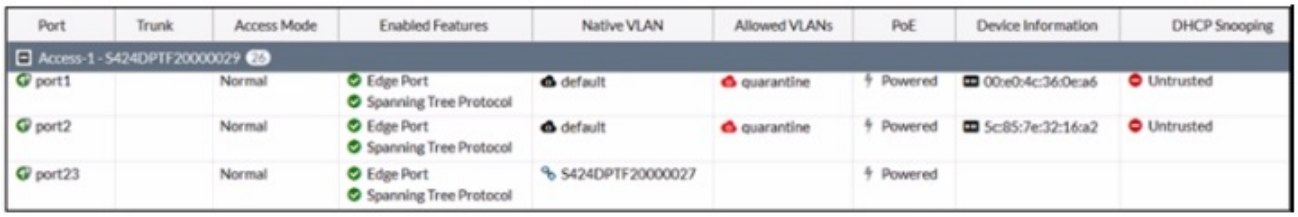
For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

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<br>Spanning Tree Protocol | default | quarantine | Powered | 00:e0:4c:36:0e:a6 | Untrusted |
| port2 | | Normal | Edge Port<br>Spanning Tree Protocol | default | quarantine | Powered | 5c:85:7e:32:16:a2 | Untrusted |
| port23 | | Normal | Edge Port<br>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?

## Options:

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.

# Question 2

Question Type: MultipleChoice

Which statement about the quarantine VLAN on FortiSwitch is true?

## Options:

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.

# Question 3

Question Type: MultipleChoice

What are two reasons why time synchronization between FortiGate and its managed FortiSwitch is critical in switch management? (Choose two.)

## Options:

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:

A, C

## 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.

# Question 4

Question Type: MultipleChoice

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.)

## Options:

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:

Based on the DHCP snooping configuration details provided in the exhibit:

B . FortiSwitch is configured to trust DHCP replies coming on FortiLink interface. The configuration segment shows 'trusted ports : port2 FlInK1 MLAG0,' indicating that the FortiSwitch is configured to trust DHCP replies coming from the specified ports, including the FortiLink interface labeled FlInK1. This setup is critical in environments where the FortiLink interface connects directly to a trusted device, such as a FortiGate appliance, ensuring that DHCP traffic on these ports is

considered legitimate.

D . Global configuration for DHCP snooping is set to forward DHCP client requests on all ports in the VLAN. The 'DHCP Broadcast Mode' set to 'All' under the DHCP Global Configuration indicates that DHCP client requests are allowed to broadcast across all ports within the VLAN. This setting is essential for environments needing broad DHCP client servicing across multiple access ports without restriction, facilitating network connectivity and management.

# Question 5

Question Type: MultipleChoice

Which LLDP-MED Type-Length-Values does FortiSwitch collect from endpoints to track network devices and determine their characteristics?

## Options:

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 the Inventory Management TLV.

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.

# Question 6

Question Type: MultipleChoice

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

## Options:

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.

## Answer:

A

## Explanation:

Fortinet FortiLink Protocol: The FortiLink protocol is Fortinet's proprietary mechanism for managing FortiSwitch units from a FortiGate firewall. It simplifies configuration and security policy enforcement across the connected network devices.

Auto-Discovery: FortiLink's auto-discovery feature means that by default, all ports on a FortiSwitch will actively send out discovery frames. This allows them to locate a FortiGate device that has a FortiLink interface enabled, streamlining the device management process.

No Configuration Needed: You don't have to manually configure individual ports for FortiLink discovery on FortiSwitch devices.

Reference

FortiSwitchOS FortiLink Guide (FortiSwitch Devices Managed by FortiOS 7.2): Refer to pages 13 and 14 for details on zero-touch management and FortiLink configuration. [https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/27f63c72-b083-11ec-9fd1-fa163e15d75b/FortiSwitchOS-7.2.0-FortiLink_Guide%E2%80%94FortiSwitch_Devices_Managed_by_FortiOS_7.2.pdf]

# Question 7

Question Type: MultipleChoice

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?

## Options:

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
D- The switch port might be used as a trunk member. When a switch port is configured as a trunk, it can carry traffic for multiple VLANs. If the sniffer is set up without specifying VLAN tags or a range of VLANs to capture, it may not accurately capture or display all the VLAN traffic due to the volume and variety of VLAN-tagged packets passing through the trunk port. This limitation makes using the sniffer on a trunk port unreliable for capturing specific VLAN traffic unless properly configured to handle tagged traffic.

## Answer:

A

## Explanation:

Page 452 of 7.2 study guide, specifically states 'Although you can use the sniffer command to capture traffic on switch ports, the types of packets capture by the sniffer are very limited.

The use of the sniffer command on FortiSwitch CLI can be unreliable on port 23 for specific reasons related to the nature of traffic on the port:

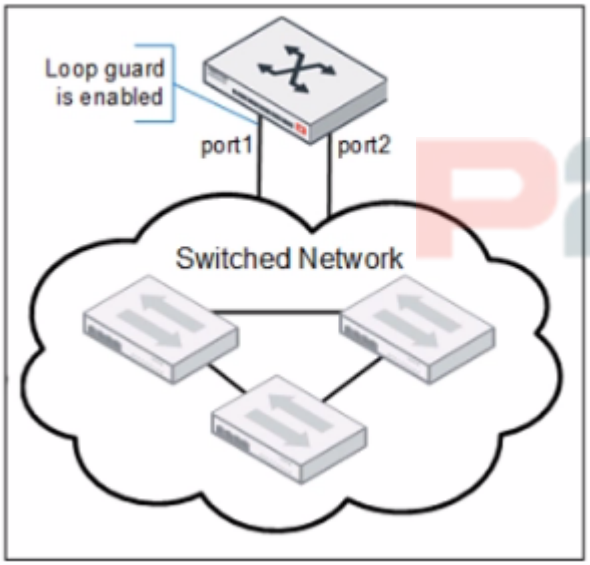
For guidelines on how to properly use sniffer commands on trunk ports and configure VLAN filtering, consult the FortiSwitch CLI reference available through Fortinet support channels, including the Fortinet Knowledge Base.

# Question 8

Question Type: MultipleChoice

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.)

## Options:

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:

A, B

## 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.

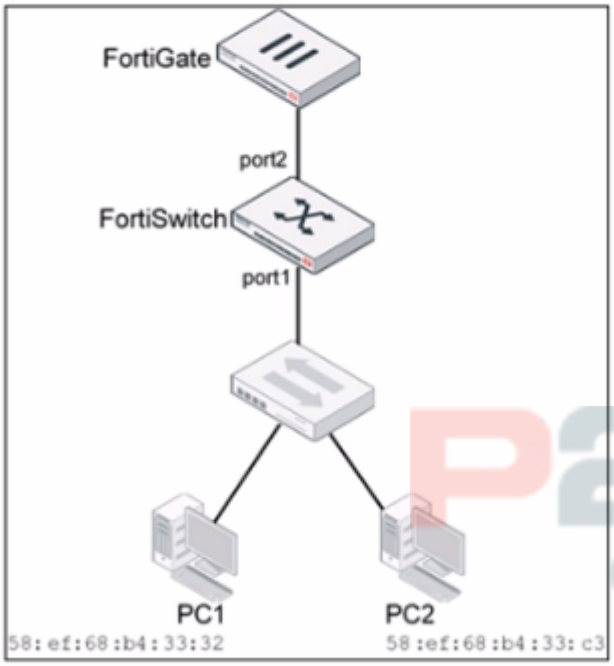
Additional details about loop guard functionality and STP interaction can be found in the FortiSwitch administration guides, accessible via Fortinet Documentation.

# Question 9

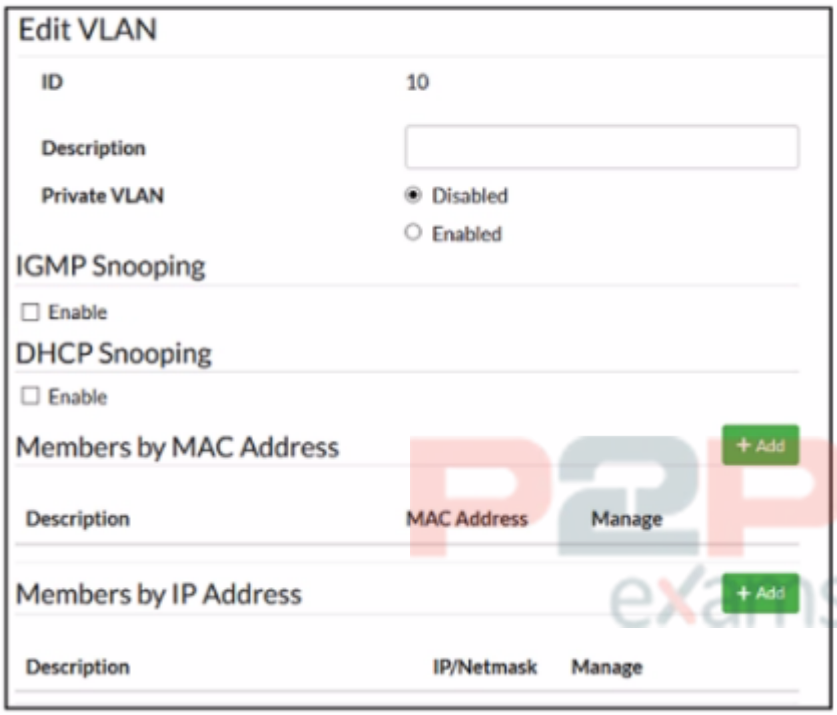
Question Type: MultipleChoice

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.)

## Options:

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:

A, B

## 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.

Fortinet FortiSwitch 7.2 Administration Guide
https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/954635/getting-started

# Question 10

Question Type: MultipleChoice

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

## Options:

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.

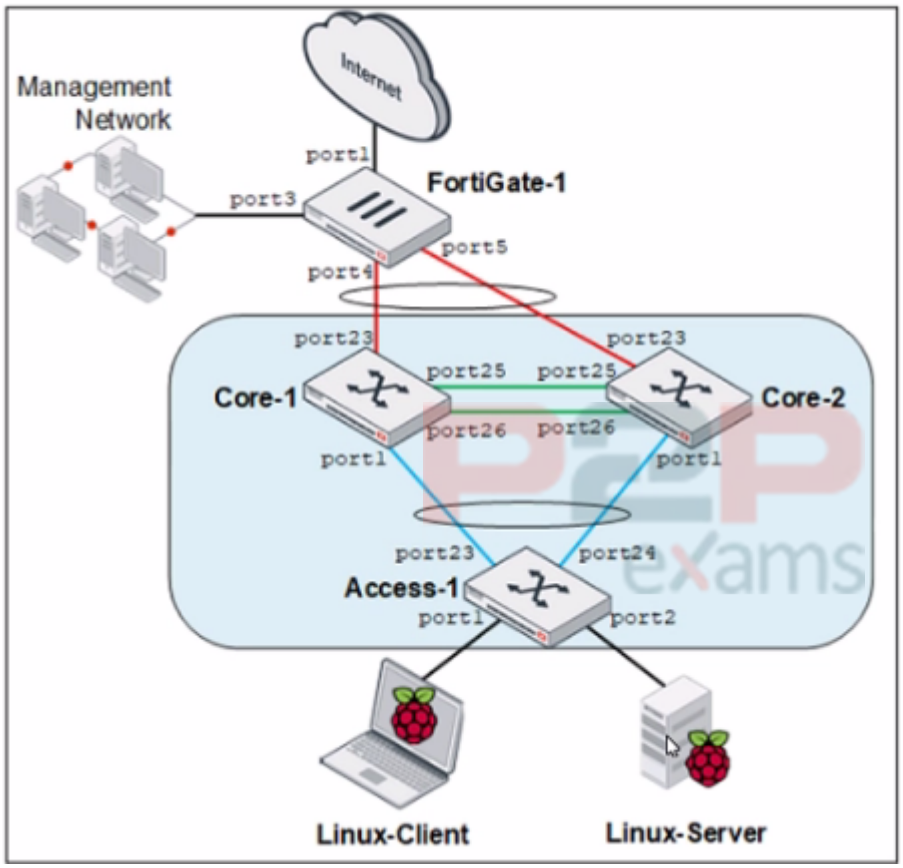
Further details on the FortiLink setup and authorization process can be accessed through the FortiGate configuration guides available on the Fortinet Documentation site.

# Question 11

Question Type: MultipleChoice

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?

## Options:

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.

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