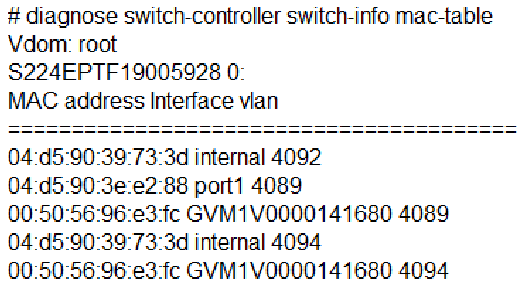
Question #1 *Topic 1*

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.

Correct Answer: *B*

Community vote distribution

B (75%) 13% 13%

shaneque 1 month ago

Selected Answer: B

La interfaz que interconecta el switch remoto y local tienen el puerto en modo TRUNK configurada con varias VLANs. Por lo tanto, se espera la dirección MAC de la interfaz en trunk se asocie con todas las VLAN incluidas. Es un comportamiento normal en switching

https://ln.run/Lga4e

upvoted 1 times

Vago_que_hace_nada 5 months, 1 week ago

Selected Answer: B

he exhibit shows the ISL to a VM Fortigate; C is not correct. Because it is the same link with the same MAC address, D is not correct; A is kind of tricky. Because it is a FortiLink indeed, but if we delete the VLANs, we will not have the scenario, and still we will have FortiLink, so A is not correct. B is the correct answer is the behavior of Fortilink configure for multiple VLANs.

Here is an example from my lab.

```
FG-01 # diagnose switch-controller switch-info mac-table | grep 84:39:8f:90:be:b2
MAC: 84:39:8f:90:be:b2  VLAN: 25 Trunk: GT80FTK23008790(trunk-id 0)
MAC: 84:39:8f:90:be:b2  VLAN: 10 Trunk: GT80FTK23008790(trunk-id 0)
MAC: 84:39:8f:90:be:b2  VLAN: 4094 Trunk: GT80FTK23008790(trunk-id 0)
```

upvoted 1 times

mkroon 5 months, 2 weeks ago

Selected Answer: A

I think A because the MAC address appears to come from a fortilink interface looking at the vlan 4093 and 4094 that are used by fortilink

upvoted 1 times

paulosrsf 7 months ago

I vote for A, because the mac address for inter-vlan routing is the mac of the gateway interace.

upvoted 2 times

Mahdi12 7 months, 2 weeks ago

Selected Answer: D

FGT Mac for all Vlan (Router on stick)

upvoted 1 times

IBB90704 9 months, 1 week ago

Selected Answer: B

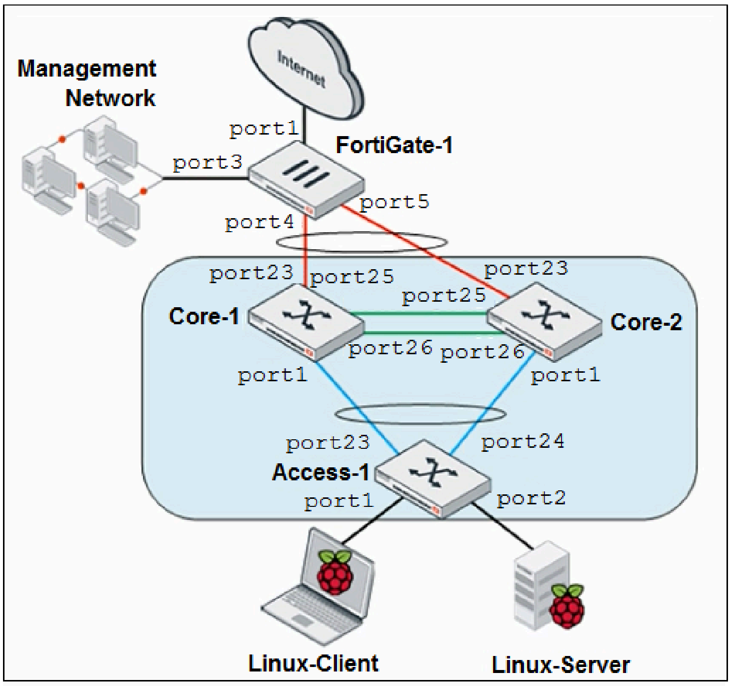
La interfaz que interconecta el switch remoto y local tienen el puerto en modo TRUNK configurada con varias VLANs. Por lo tanto, se espera la dirección MAC de la interfaz en trunk se asocie con todas las VLAN incluidas. Es un comportamiento normal en switching

upvoted 4 times

Question #2 *Topic 1*

Refer to the exhibit.

MCL-Topology



Core-1 and Access-1 are managed and authorized by FortiGate-1, which uses port4 as the FortLink 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.

Correct Answer: *B*

Community vote distribution

B (100%)

67e86f5 10 months ago

Selected Answer: B

Answer is B

upvoted 4 times

Question #3 *Topic 1*

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. Fortiink frame is sent by FortiGate to FortiSwitch to complete the authorization.

D. FortiLink authorization sets the FortiSwitch management mode to FortiLink.

Correct Answer: *CD*

Community vote distribution

CD (100%)

herlock_sholmes_2810 8 months, 4 weeks ago

Selected Answer: CD

B. FortiSwitch requires a reboot to complete the authorization process. [WRONG]
"When you change the management mode of FortiSwitch, the switch does not reboot." page 11

C. FortiLink frame is sent by FortiGate to FortiSwitch to complete the authorization. [CORRECT]
"4. FortiGate sends a FortiLink frame to the switch to notify that it has been authorized." page 25

D. FortiLink authorization sets the FortiSwitch management mode to FortiLink. [CORRECT]
"6. FortiSwitch changes to FortiLink mode." page 26

Reference: FortiSwitch 7.2 Study Guide

upvoted 2 times

IBB90704 9 months, 1 week ago

Selected Answer: CD

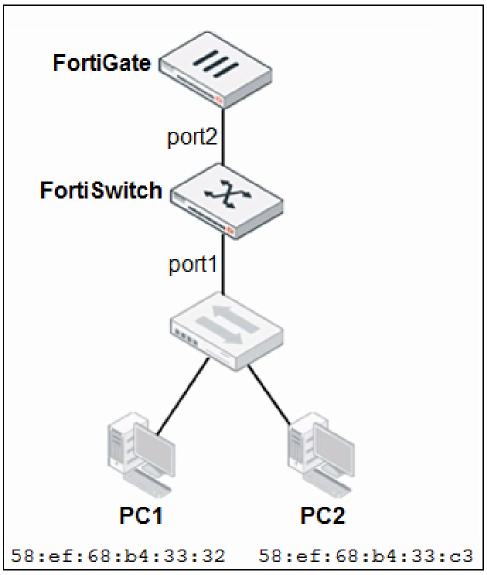
Leer pagina 25 y 26 del libro FortiSwitch 7.2 Study Guide

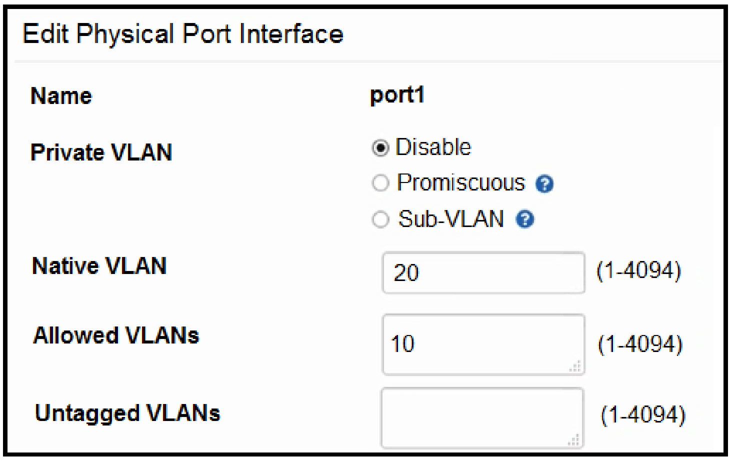
upvoted 4 times

Question #4 *Topic 1*

Refer to the exhibits.

Topology





Edit Physical Port Interface

Name port1

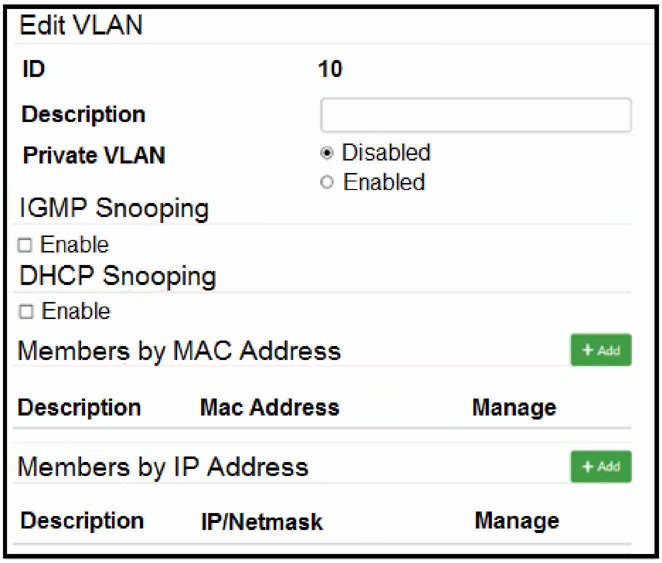
Private VLAN ● Disable ○ Promiscuous ○ Sub-VLAN

Native VLAN 20 (1-4094)

Allowed VLANs 10 (1-4094)

Untagged VLANs (1-4094)

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 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.

Correct Answer: *AB*

Community vote distribution

AB (100%)

herlock_sholmes_2810 9 months ago

Selected Answer: AB

A. Add the MAC address of PC1 as a member of VLAN 10.

When receives untagged frame, Member by MAC adds tag to the frame. (page 376)

B. Add VLAN ID 10 as a member of the untagged VLANs on port1.

Because, when the switch receives tagged frame to VLAN 10, it forwarded without tag, thats what PC1 expected. (page 121)

upvoted 1 times

herlock_sholmes_2810 9 months ago

But I agree that the question is wrong. "Which two configurations can you perform on fsw to ENSURE pc1 receives untagged traffic on port1?"

Based in this question, letter A doesn't make sense.

upvoted 1 times

JustWondering 9 months, 1 week ago

Selected Answer: AB

correct answers according to study guide.

upvoted 3 times

IBB90704 9 months, 2 weeks ago

La respuesta es la A y la B. Leer pagina 121 y 376 del libro

upvoted 3 times

67e86f5 9 months, 2 weeks ago

This is a poorly phrased question .. the study guide doesn't really give a good answer for this one. Anyone?

upvoted 3 times

Christiandus 9 months, 3 weeks ago

B is correct, however all other answers seem wrong?

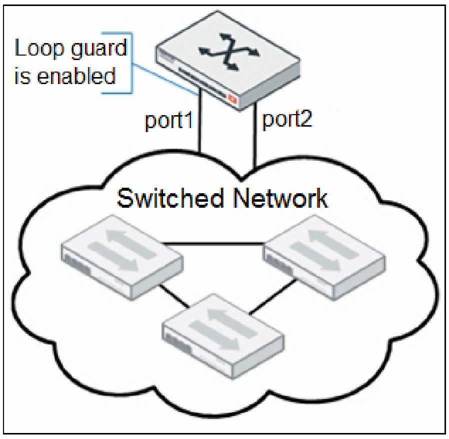
C: Should be incorrect according to study guide page 121 "For the setting to take effect, the untagged VLAN must also be a member of the allowed VLAN list."

upvoted 2 times

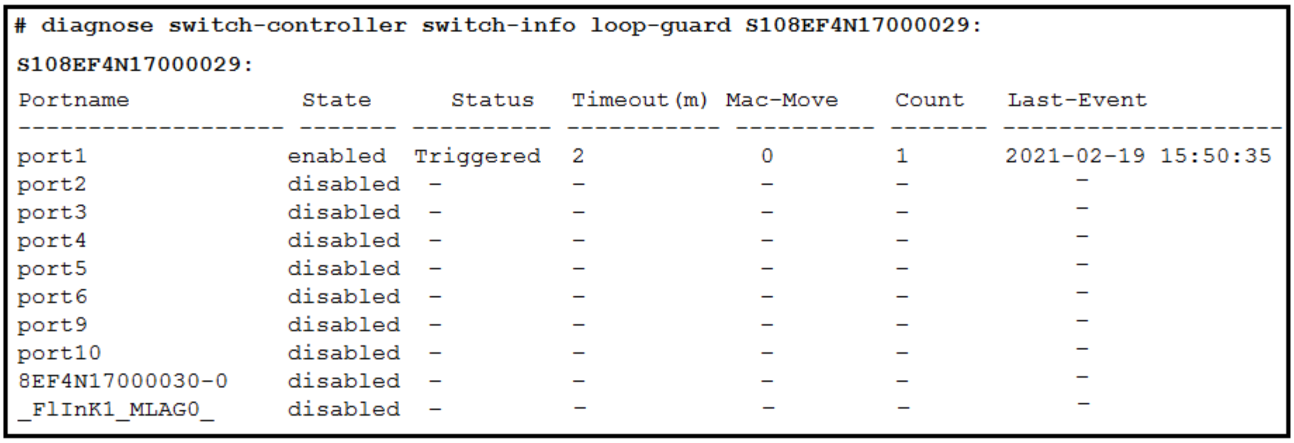
Question #5 *Topic 1*

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.)

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 port1 was received on port1.

Correct Answer: *AD*

Community vote distribution

AD (71%) AC (29%)

Vago_que_hace_nada 5 months ago

Selected Answer: AD

C couldn't be a correct answer because BPDUs (Bridge Protocol Data Units) are generally sent by switches and not typical endpoint devices like PCs, IP phones, cameras, or printers.

upvoted 1 times

oriollorenzo 7 months, 3 weeks ago

Selected Answer: AD

A & D.

C is bpdu guard, not loop guard.

upvoted 2 times

e93df3f 7 months, 3 weeks ago

A & C check the script

upvoted 2 times

⊟ **GPFT** 8 months, 3 weeks ago

Selected Answer: AD

La respuesta es la A y D

D: pag 200, párrafo 3 "FortiSwitch then shuts down port 1 if it receives a loop guard frame sourced from port1 on either port1 or port2"

upvoted 2 times

⊟ **IBB90704** 9 months, 1 week ago

Selected Answer: AC

La respuesta es las A y C leer pagina 200

upvoted 2 times

⊟ **Vago_que_hace_nada** 5 months ago

Los endpoint (PCs, Printers, Telefonos IP, etc) no envia BPDUs por esa razon C no es correcta. Ademas la pagina 200 dice que Loop Gard no depende de BPDUs.

upvoted 1 times

⊟ **JustWondering** 9 months, 1 week ago

A and C look correct.

upvoted 2 times

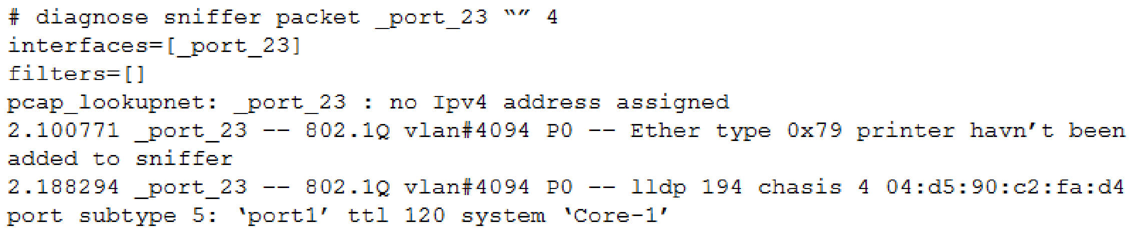
⊟ **IBB90704** 9 months, 2 weeks ago

La respuesta es las A y C leer pagina 200

upvoted 2 times

Question #6 *Topic 1*

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 chasis 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.

Correct Answer: *A*

Community vote distribution

A (100%)

herlock_sholmes_2810 9 months ago

Selected Answer: A

A. The types of packets captured is limited.

Reference: FortiSwitch 7.2 Study Guide, page 452 (Troubleshooting > Packet Capture)

upvoted 2 times

JustWondering 9 months, 1 week ago

Selected Answer: A

A is correct

upvoted 4 times

JustWondering 9 months, 3 weeks ago

Answer is A.

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.

upvoted 3 times

Question #7 *Topic 1*

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

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 by default.

Correct Answer: *A*

Community vote distribution

A (93%) 7%

jomzilla17 5 months, 4 weeks ago

Selected Answer: B

Answer is B

upvoted 1 times

herlock_sholmes_2810 9 months, 1 week ago

Selected Answer: A

A. "Every FortiSwitch broadcasts FortiLink discovery frames on all ports, by default."

Reference: FortiSwitch 7.2 Study Guide, page 22

upvoted 4 times

IBB90704 9 months, 1 week ago

Selected Answer: A

La respuesta es la A leer la pagina 22

upvoted 3 times

JustWondering 9 months, 1 week ago

Selected Answer: A

A is correct as seen in the study guide

upvoted 3 times

IBB90704 9 months, 2 weeks ago

La respuesta es la A leer la pagina 22

upvoted 3 times

greeklover84 9 months, 3 weeks ago

Selected Answer: A

Correct Answer is A. checked it on the Study book.

upvoted 3 times

Question #8 *Topic 1*

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

Correct Answer: *D*

Community vote distribution

D (100%)

⊟ **herlock_sholmes_2810** 9 months, 1 week ago

Selected Answer: D

D) "Inventory management: FortiSwitch collects detailed information about endpoints, enabling network administrators to track their network devices and determine their characteristics."

Reference: FortiSwitch 7.2 Study Guide, page 290

upvoted 4 times

⊟ **IBB90704** 9 months, 1 week ago

Selected Answer: D

La respuesta es la D leer pagina 290

upvoted 2 times

⊟ **JustWondering** 9 months, 1 week ago

Selected Answer: D

D is correct according to study guide

upvoted 2 times

⊟ **IBB90704** 9 months, 2 weeks ago

La respuesta es la D leer pagina 290

upvoted 2 times

⊟ **greeklover84** 9 months, 3 weeks ago

Selected Answer: D

D. I checked it in the study book.

upvoted 2 times

⊟ **67e86f5** 10 months, 1 week ago

Selected Answer: D

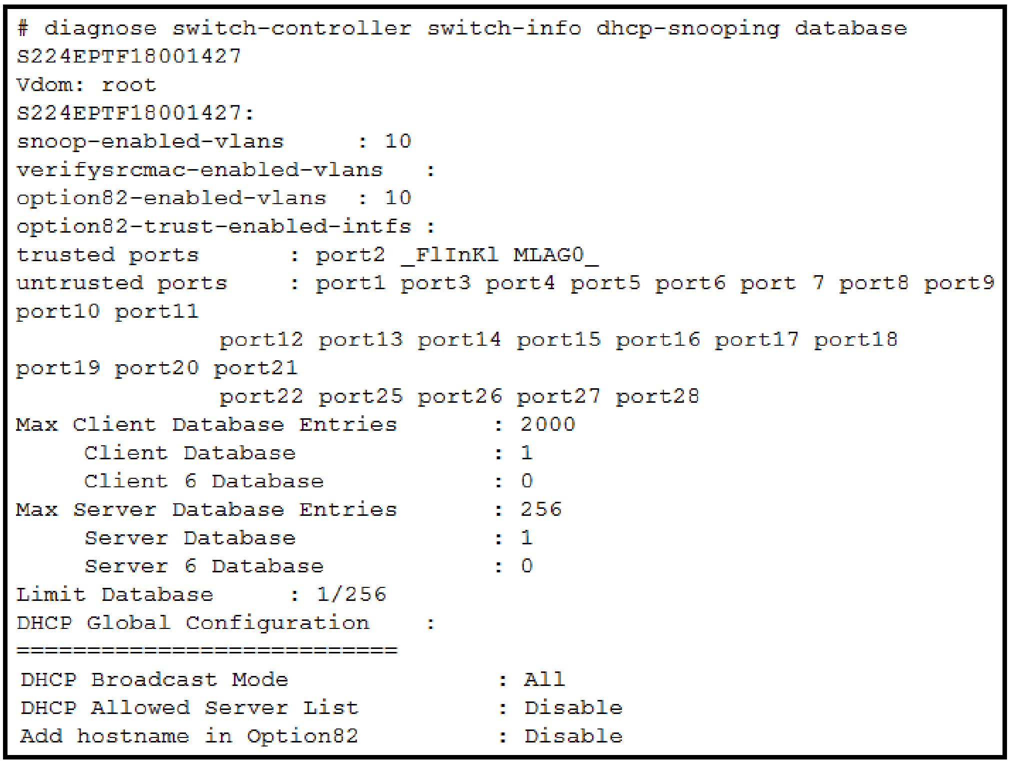
Answer is D

upvoted 4 times

Question #9 Topic 1

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 _FlInKl MLAG0_
untrusted ports     : port1 port3 port4 port5 port6 port 7 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
     Client 6 Database             : 0
Max Server Database Entries        : 256
     Server Database               : 1
     Server 6 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.)

A. Maximum value to accept clients DHCP request is configured as per DHCP server range.

B. Fortiswitch is configured to trust OHCP replies coming on FortLink 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.

Correct Answer: *BD*

Community vote distribution

BD (100%)

herlock_sholmes_2810 9 months ago

Selected Answer: BD

B. FortiSwitch is configured to trust DHCP replies coming on FortLink interface.

```trusted ports: port2 _Flinkl MLAG0_```

D. Global configuration for DHCP snooping is set to forward DHCP client requests on all ports in the VLAN.

```DHCP Broadcas Mode : All```

Reference: FortiSwitch 7.2 Study Guide, page 217

upvoted 3 times

JustWondering 9 months, 1 week ago

Selected Answer: BD

B and D are correct

upvoted 3 times

67e86f5 10 months, 1 week ago

Selected Answer: BD

Answer is B and D

upvoted 3 times

Question #10 Topic 1

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.

Correct Answer: *AC*

Community vote distribution

AC (100%)

⊟ **herlock_sholmes_2810** 9 months, 1 week ago

Selected Answer: AC

"Time synchronization is critical in switch management. If the time on FortiGate and FortiSwitch is not synchronized, FortiSwitch can't complete the DTLS handshake used in CAPWAP, which prevents the switch from connecting to FortiGate. Another reason to have a working setup for time synchronization is because FortiSwitch doesn't retain its time after a reboot. When FortiSwitch is rebooted, the time on the switch is reset to the Unix epoch time (midnight of January 1, 1970, UTC)."

Reference: FortiSwitch 7.2 Study Guide, page 413

upvoted 4 times

⊟ **JustWondering** 9 months, 1 week ago

Selected Answer: AC

A and C are correct

upvoted 2 times

⊟ **67e86f5** 10 months ago

Selected Answer: AC

Answer is A and C

upvoted 4 times

Question #11 *Topic 1*

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.

Correct Answer: *B*

Community vote distribution

B (100%)

herlock_sholmes_2810 9 months ago

Selected Answer: B

B. Because you CAN (not must) place devices that try to authenticate through 802.1X, but fail, in the VLAN selected as Authentication fail VLAN. In the example image of the Study Guide, they used quarantined VLAN for this option.

Reference: FortiSwitch 7.2 Study Guide, page 232

upvoted 2 times

JustWondering 9 months, 1 week ago

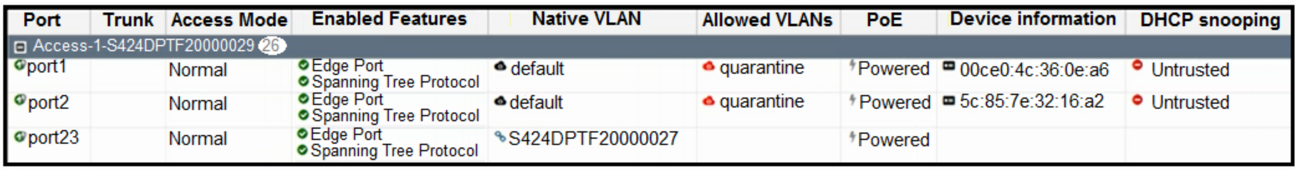
Selected Answer: B

B is correct.

upvoted 3 times

Question #12 *Topic 1*

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	00ce0:4c: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.

Correct Answer: *B*

Community vote distribution

B (100%)

⊟ **7ab89e0** 1 month, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

Question #13 *Topic 1*

What are two ways in which automatic MAC address quarantine works on FortiSwitch? (Choose two.)

A. FortiSwitch supports only by VLAN quarantine mode.

B. FortiGate applies the quarantine-related configuration only on FortiGate.

C. FortiAnalyzer with a threat detection services license is required.

D. MAC address quarantine can be enabled through the FortiGate CLI only.

Correct Answer: *CD*

Community vote distribution

CD (100%)

herlock_sholmes_2810 8 months, 4 weeks ago

Selected Answer: CD

A. FortiSwitch supports only by VLAN quarantine mode. [WRONG]
"FortiGate/FortiSwitch supports two MAC address quarantine modes: by VLAN and by redirect."

B. FortiGate applies the quarantine-related configuration only on FortiGate. [WRONG]
"FortiGate applies the quarantine-related configuration for the quarantined device to FortiSwitch using the FortiSwitch REST API."

C. FortiAnalyzer with a threat detection services license is required. [CORRECT]
D. MAC address quarantine can be enabled through the FortiGate CLI only. [CORRECT]
"Note that automatic quarantine requires a FortiAnalyzer device with a valid threat detection services license. To enable MAC address quarantine on the FortiGate CLI."

Reference: FortiSwitch 7.2 Study Guide, page 263

upvoted 4 times

greeklover84 9 months, 3 weeks ago

Selected Answer: CD

C,D have checked it in the book.

upvoted 4 times

Question #14 *Topic 1*

How does FortiGate handle configuration of flow tracking sampling if you export the settings to a managed FortiSwitch stack with sampling mode set to perimeter is true?

A. FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces.

B. FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces.

C. FortiGate configures and enables flow sampling on FortiSwitch but does not change existing sampling settings of interfaces

D. FortiGate configures and enables egress sampling on all management interfaces.

Correct Answer: *B*

Community vote distribution

B (100%)

herlock_sholmes_2810 9 months, 2 weeks ago

Based on FortiSwitch 7.2 Study Guide:

"perimeter: FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces."

on page 324.

upvoted 2 times

herlock_sholmes_2810 9 months, 2 weeks ago

Selected Answer: B

Based on FortiSwitch 7.2 Study Guide:

"perimeter: FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces."

on page 324.

upvoted 2 times

herlock_sholmes_2810 8 months, 4 weeks ago

Just for notation:

A. FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces. [WRONG]
Incomplete.

B. FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces. [CORRECT]
This is PERIMETER sampling mode.

C. FortiGate configures and enables flow sampling on FortiSwitch but does not change existing sampling settings of interfaces. [WRONG]
This is LOCAL sampling mode.

D. FortiGate configures and enables egress sampling on all management interfaces. [WRONG]
That's incorrect.
|
v
"FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces." that's DEVICE-INGRESS sampling mode.

upvoted 2 times

67e86f5 9 months, 2 weeks ago

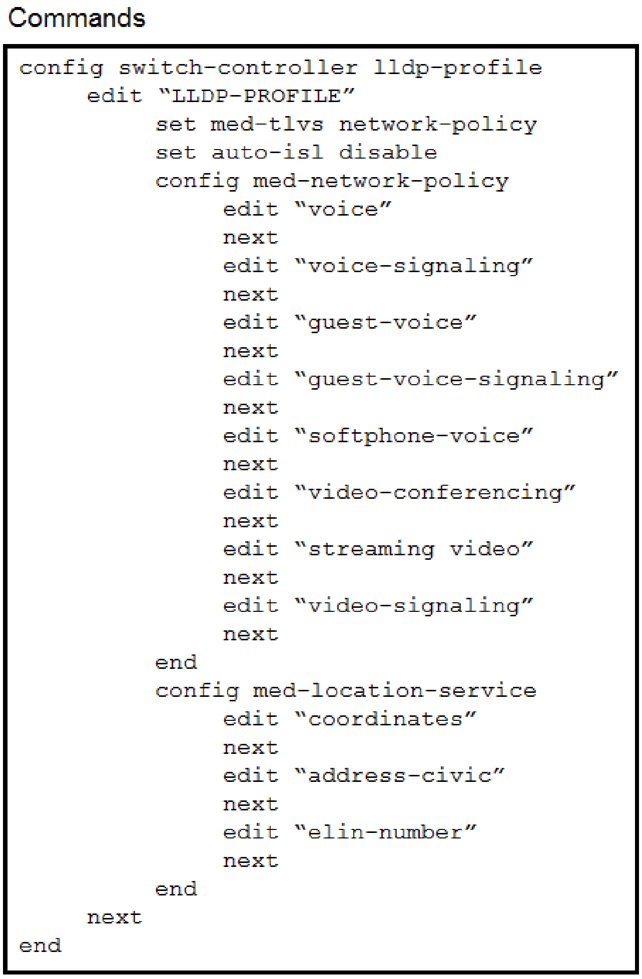
Selected Answer: B

FortiSwitch Study Guide 7.2 page 324

upvoted 4 times

Question #15 Topic 1

Refer to the exhibit.



Commands

```
config switch-controller lldp-profile
     edit “LLDP-PROFILE”
          set med-tlvs network-policy
          set auto-isl disable
          config med-network-policy
               edit “voice”
               next
               edit “voice-signaling”
               next
               edit “guest-voice”
               next
               edit “guest-voice-signaling”
               next
               edit “softphone-voice”
               next
               edit “video-conferencing”
               next
               edit “streaming video”
               next
               edit “video-signaling”
               next
          end
          config med-location-service
               edit “coordinates”
               next
               edit “address-civic”
               next
               edit “elin-number”
               next
          end
     next
end
```

The profile shown in the exhibit is assigned to a group of managed FortiSwitch ports, and these ports are connected to endpoints which are powered by PoE.

Which configuration action can you perform on the LLDP profile to cause these endpoints to exchange PoE information and negotiate power with the managed FortiSwitch?

A. Create new a LLDP-MED application type to define the PoE parameters.

B. Assign a new LDP profile to handle different LLDP-MED TLVs.

C. Define an LLDP-MED location ID to use standard protocols for power.

D. Add power management as part of LLDP-MED TLVs to advertise.

Correct Answer: *D*

Community vote distribution

D (100%)

Vago_que_hace_nada 5 months ago

Selected Answer: D

Here is the snippet:

HA-01 (LLDP-PROFILE) # set med-tlvs

inventory-management Inventory management TLVs.

network-policy Network policy TLVs.

power-management Power manangement TLVs.

location-identification Location identificaion TLVs.

HA-01 (LLDP-PROFILE) # set med-tlvs power-management

upvoted 1 times

⊟ **wsdeffwd** 8 months, 3 weeks ago

Selected Answer: D

Page 291

upvoted 3 times

Question #16 *Topic 1*

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

Correct Answer: *BC*

Community vote distribution

BC (100%)

herlock_sholmes_2810 Highly Voted 👍 9 months, 1 week ago

Selected Answer: BC

"You can configure Layer 3 interfaces to perform routing on FortiSwitch. The following types of Layer 3 interfaces are supported: Loopback [...] Switch virtual interface (SVI)".

Reference: FortiSwitch 7.2 Study Guide, page 385.

upvoted 7 times

JustWondering Highly Voted 👍 9 months, 1 week ago

Selected Answer: BC

page 385 of study guide 7.2

upvoted 6 times

Question #17 *Topic 1*

What feature can network administrators use to segment network operations and the administration of managed FortiSwitch devices on FortiGate?

A. FortiGate multi-tenancy

B. Multi-chassis links aggregation trunk

C. FortiGate clustering protocol

D. FortiLink split interface

Correct Answer: *A*

Community vote distribution

A (100%)

JustWondering 9 months, 1 week ago

Selected Answer: A

A is correct

upvoted 3 times

herlock_sholmes_2810 9 months, 2 weeks ago

Selected Answer: A

A) FortiGate multi-tenancy

Reference: "FortiSwitch 7.2 Study Guide" page 299

upvoted 2 times

67e86f5 9 months, 3 weeks ago

Selected Answer: A

It is A. FortiGate Multi Tenancy is vDOMs

upvoted 2 times

greeklover84 9 months, 3 weeks ago

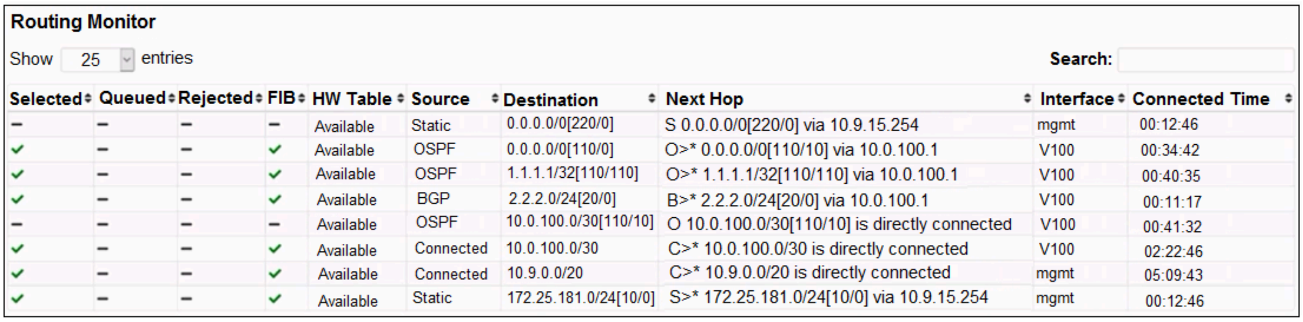
Selected Answer: A

why not A ?

upvoted 3 times

Question #18 *Topic 1*

Refer to the exhibit.



Routing Monitor

Show 25 entries **Search:**

Selected	Queued	Rejected	FIB	HW Table	Source	Destination	Next Hop	Interface	Connected Time
–	–	–	–	Available	Static	0.0.0.0/0[220/0]	S 0.0.0.0/0[220/0] via 10.9.15.254	mgmt	00:12:46
✓	–	–	✓	Available	OSPF	0.0.0.0/0[110/0]	O>* 0.0.0.0/0[110/10] via 10.0.100.1	V100	00:34:42
✓	–	–	✓	Available	OSPF	1.1.1.1/32[110/110]	O>* 1.1.1.1/32[110/110] via 10.0.100.1	V100	00:40:35
✓	–	–	✓	Available	BGP	2.2.2.0/24[20/0]	B>* 2.2.2.0/24[20/0] via 10.0.100.1	V100	00:11:17
–	–	–	–	Available	OSPF	10.0.100.0/30[110/10]	O 10.0.100.0/30[110/10] is directly connected	V100	00:41:32
✓	–	–	✓	Available	Connected	10.0.100.0/30	C>* 10.0.100.0/30 is directly connected	V100	02:22:46
✓	–	–	✓	Available	Connected	10.9.0.0/20	C>* 10.9.0.0/20 is directly connected	mgmt	05:09:43
✓	–	–	✓	Available	Static	172.25.181.0/24[10/0]	S>* 172.25.181.0/24[10/0] via 10.9.15.254	mgmt	00:12:46

Two routes are not installed in the forwarding information base (FIB) as shown in the exhibit.

Which two statements about these two route entries are true? (Choose two.)

A. These two routes have a higher administrative distance value available to the destination networks.

B. These two routes will be used as load-balancing routes.

C. These two routes will become primary, if the best routes are removed.

D. These two routes are available in the hardware routing table.

Correct Answer: *CD*

Community vote distribution

CD (78%) AC (22%)

7ab89e0 1 month, 1 week ago

Selected Answer: CD

Answer is C and D per page 393 of the FortiSwitch 7.2 Study Guide

upvoted 1 times

M33 7 months, 2 weeks ago

Selected Answer: CD

In both cases, the administrative distance is smaller.

First case 220(static) Vs110(OSPF)

Second Case 110(OSPF) 0(Directly connected)

Although the distance of the directly connected route does not appear in the table (even if we look at a FortiGate in the GUI we will see that it is 0)

However, the official guide on page 393 also tells us that these entries are available in the Hardware Table, which the FortiSwitch uses.

Option C also seems correct.

I am a little confused with this question because all three options seem valid.

upvoted 3 times

IBB90704 9 months, 1 week ago

Selected Answer: AC

Pagina 393 del libro FortiSwitch 7.2 Study Guide

La desicion de enrutamiento en el Fortiswitch puede ser basado en hardware donde se usa las rutas en la tabla de enrutamiento de hardware, que se cargan en el ASIC. El enrutamiento basado en software se realiza cuando FortiSwitch usa las rutas en la FIB, que se cargan en el núcleo.

En el ejemplo que se muestra en esta diapositiva, la primera ruta de la tabla, que es una ruta estática predeterminada con una distancia de
220, no está instalada en la FIB porque FortiSwitch prefirió la ruta predeterminada aprendida a través de OSPF, que
tiene una distancia menor (110). Sin embargo, la ruta estática permanece en espera y se instala en la FIB si se elimina la ruta
OSPF

upvoted 1 times

herlock_sholmes_2810 9 months, 1 week ago

Selected Answer: CD

I think thats the correct answers are C and D.

C. These two routes will become primary, if the best routes are removed. > Thats because the Selected column is unmarked, so thats isn't the best route, but if the primary route get close, these routes will come up.

D. These two routes are available in the hardware routing table. > Thats is obvious seen the HW Table column, that shows Available, which means that these routes are installed in the hardware routing table.

Reference: FortiSwitch 7.2 Study Guide, page 393.

upvoted 3 times

⊟ **JustWondering** 9 months, 1 week ago

Selected Answer: AC

A and C are def correct.

upvoted 1 times

Question #19 *Topic 1*

Which packet capture method allows FortiSwitch to capture traffic on trunks and management interfaces?

A. SPAN

B. Sniffer profile

C. sFlow

D. TCP dump

Correct Answer: *B*

Community vote distribution

B (88%) 13%

herlock_sholmes_2810 9 months ago

Selected Answer: B

B. FortiSwitch 7.2 Study Guide, page 448

upvoted 1 times

IBB90704 9 months, 1 week ago

Selected Answer: B

Leer pagina 448 del FortiSwitch 7.2 Study Guide.

En la tabla muestra los diferentes Packet Capture Method a escojer donde solo el Sniffer profile cumple

upvoted 1 times

IBB90704 9 months, 1 week ago

Selected Answer: B

Leer pagina 448 del FortiSwitch 7.2 Study Guide.

En la tabla muestra los diferentes Packet Capture Method a escojer donde solo el Sniffer profile cumple

upvoted 1 times

herlock_sholmes_2810 9 months, 2 weeks ago

B) Sniffer profile can capture in internal, mgmt, switch ports and trunks interfaces.

upvoted 1 times

67e86f5 9 months, 2 weeks ago

Selected Answer: B

I just double checked. It's definitely B. FortiSwitch Study Guide 7.2 page 448

upvoted 2 times

67e86f5 9 months, 3 weeks ago

Selected Answer: B

I think it's B. Sniffer Profile can capture mgmt interface traffic and vlans.

upvoted 2 times

greeklover84 9 months, 3 weeks ago

Selected Answer: C

it is c.

upvoted 1 times

herlock_sholmes_2810 9 months, 2 weeks ago

I think that B) because it asks "capture traffic on trunks AND management interface".
sFlow, according to FortiSwitch 7.2 Study Guide, can capture internal, switch ports, trunks and multiple, not mgmt.

FortiSwitch 7.2 Study Guide page 448

upvoted 1 times

Question #20 *Topic 1*

Which Ethernet frame can create Layer 2 flooding due to all bytes on the destination MAC address being set to all FF?

A. The broadcast Ethernet frame

B. The unicast Ethernet frame

C. The multicast Ethernet frame

D. The anycast Ethernet frame

Correct Answer: *A*

Community vote distribution

A (100%)

herlock_sholmes_2810 9 months ago

Selected Answer: A

A. The broadast Ethernet frame

FF:FF:FF:FF:FF:FF > Frame destined to all devices (broadcast)

upvoted 3 times

IBB90704 9 months, 1 week ago

Selected Answer: A

Leer pagina 75 del FortiSwitch 7.2 Study Guide

upvoted 4 times

Question #21 *Topic 1*

Which is a requirement to enable SNMP v2c on a managed FortiSwitch?

A. Create a SNMP user to use for authentication and encryption.

B. Specify an SNMP host to send traps to.

C. Enable an SNMP v3 to handle traps messages with SNMP hosts.

D. Configure SNMP agent and communities.

Correct Answer: *D*

Community vote distribution

D (100%)

⊟ **herlock_sholmes_2810** 9 months ago

Selected Answer: D

A. Create a SNMP user to use for authentication and encryption. [WRONG]
Because authentication and encryption is for SNMPv3.

B. Specify a SNMP host to send traps to. [WRONG]
Because you can use SNMP v2c without a specified host, but won't send any SNMP traps.

C. Enable an SNMP v3 to handle traps messages with SNMP hosts. [WRONG]
This is for SNMPv3.

D. Configure SNMP agent and communities. (CORRECT)

upvoted 3 times

⊟ **IBB90704** 9 months, 1 week ago

Selected Answer: D

Leer pagina 311 y 312 del FortiSwitch 7.2 Study Guide

-he first
step is to enable SNMP access on the internal interface by either changing the default local access profile or
creating a new one.
- The second step is to enable the SNMP agent and configure the SNMP common settings,
- After you enable the SNMP agent and configure SNMP common settings, you must create one or more
SNMP communities

upvoted 3 times

Question #22 *Topic 1*

What can an administrator do to maintain a Forti-Gate-compatible FortiSwitch configuration when changing the management mode from standalone to FortiLink?

A. Use a migration tool based on Python script to convert the configuration.

B. Enable the FortiLink setting on FortiSwitch before the authorization process.

C. FortiGate automatically saves the existing FortiSwitch configuration during the FortiLink management process.

D. Register FortiSwitch to FortiSwitch Cloud to save a copy before managing with FortiGate.

Correct Answer: *A*

Community vote distribution

A (100%)

herlock_sholmes_2810 9 months ago

Selected Answer: A

"The tool is a Python script that converts the supported settings in a FortiSwitch standalone configuration file to the equivalent FortiOS settings for a managed switch."

Reference: FortiSwitch 7.2 Study Guide, page 349

upvoted 1 times

IBB90704 9 months, 1 week ago

La respuesta no esta en el libro pero se podria utilizar Python script o forticonverter ambas son viables para convertir configuraciones.

Asi que la respuestas es la A

upvoted 3 times

67e86f5 9 months, 2 weeks ago

Selected Answer: A

Answer is A. Reference "FortiLink Guide - FortiSwitch Devices Managed by FortiOS 7.2" page 25

upvoted 4 times