Free Questions for NSE6_FSW-7.2 by dumpshq

Shared by Rice on 09-08-2024

For More Free Questions and Preparation Resources

Question 1

Which drop policy mode, if assigned to a congested port, will drop incoming packets until there is no congestion on the egress port?

Options:

A- Tail-drop mode

B- Weighted round robin mode.

C- Random early detection mode
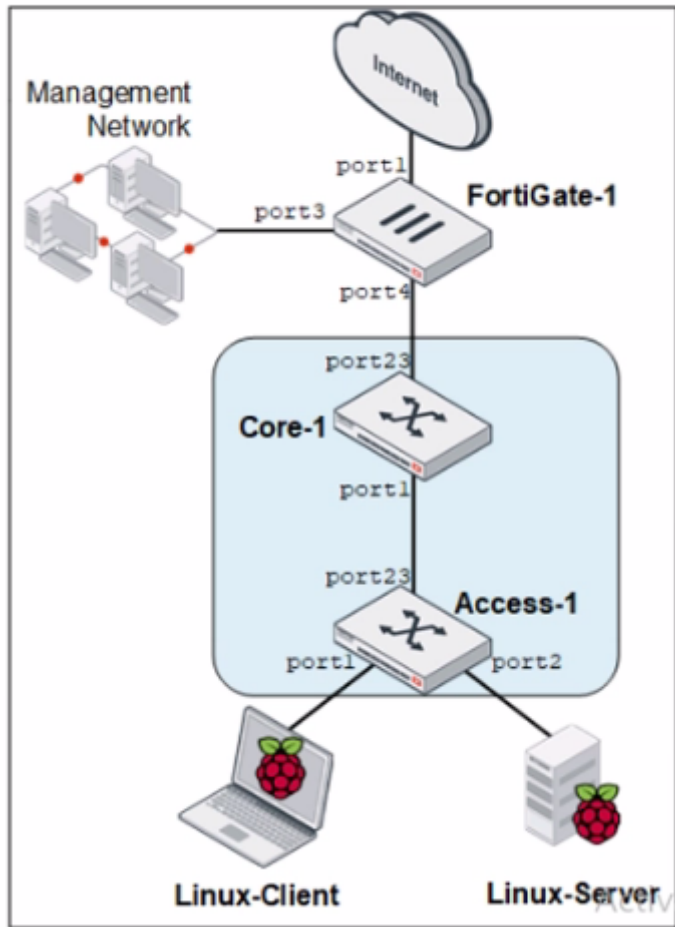
D- Strict mode

Answer:

A

Question 2

Refer to the exhibits.

Topology

Address

IP/Netmask	169.254.1.1/255.255.255.0
Connected devices	0 FortiSwitch(es)
Automatically authorize devices ⓘ ⬤	
FortiLink split interface ⓘ ⬤	
IoT scanning ⓘ ⬤	

⬤ DHCP Server

Address range	169.254.1.2-169.254.1.254
	➕
Netmask	255.255.255.0
Default gateway	Same as Interface IP Specify
DNS server	Same as System DNS Same as Interface IP Specify 0.0.0.0
Lease time ⓘ ⬤	604800 second(s)

➕ Advanced

⬤ NAC Settings

Traffic Shaping

Outbound shaping profile ⬤	

Miscellaneous

Comments	0/255
Status	➕ Enabled ➖ Disabled

You are asked to ensure that managed FortiSwitch devices are reachable by other devices, such as SNMP and other management tools across your network.

Which setting must you configure to ensure traffic from other devices in the network reaches FortiSwitch?

Options:

A- Select a specific default gateway provided to FortiSwitch as an upstream device.

B- Change the FortiLink interface IP address and DHCP server address range.

C- Recreate the FortiLink interface with a nonaggregate setting.

D- Enable NAC settings to select the onboarding VLAN.

Answer:

B

Question 3

Question Type: MultipleChoice

Which statement about 802.1X security profiles using MAC-based authentication mode is true?

Options:

A- FortiSwitch allows connectivity to all hosts connected to a port, if one host is authenticated.

B- FortiSwitch can grant each device a different access level based on the credentials provided

C- FortiSwitch performs faster when using this security mode on the ports.

D- FortiSwitch must communicate with the RADIUS server to authenticate devices

Answer:

B

Question 4

Question Type: **MultipleChoice**

Which QoS mechanism maps packets with specific CoS or DSCP markings to an egress queue?

Options:

A- Queuing for egress traffic

B- Classification for ingress traffic

C- Rate limiting for egress traffic

D- Marking for ingress traffic

Answer:

B

Question 5

Refer to the configuration:

```
config switch phy-mode
set port-configuration disable-port54
set port53-phy-mode 4x10G
end
```

Which two conditions does FortiSwitch need to meet to successfully configure the options shown in the exhibit above? (Choose two.)

Options:

A- The FortiSwitch model is equipped with a maximum of 54 interfaces

B- FortiSwitch would need to be rebooted.

C- The split port can be assigned to a native VLAN.

D- The Dort full speed prior to the split was 100G QSFP+.

Question 6

Question Type: **MultipleChoice**

Which two rules used by MSTP are similar to rules used by other STP methods? (Choose two.)

Options:

A- MSTP uses port role election, similar to rapid STP on the instances.

B- MSTP uses alternate path and primary path, similar to regular STP.

C- MSTP uses root bridge selection, similar to rapid STP

D- MSTP uses timers for transitioning the ports, similar to regular STP.

Answer:

B, C

Question 7

Which two statements about VLAN assignments on FortiSwitch ports are true? (Choose two.)

Options:

A- Configure a native VLAN on the FortiLink

B- Assign an IP address and subnet mask to FortiSwitch VLANs

C- Only assign one native VLAN on a port

D- Assign untagged VLANs using FortiGate CLI

Answer:

C, D

Question 8

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.)

Options:

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:

A, B

Question 9

Question Type: **MultipleChoice**

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

Options:

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.

Answer:

D