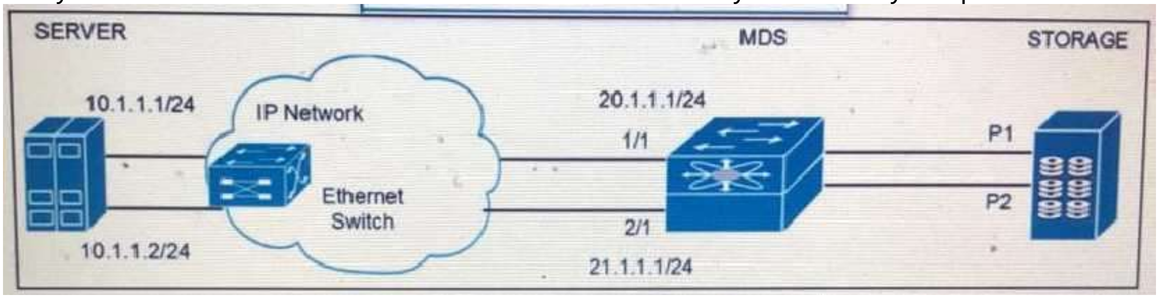
QUESTION 117

Refer to the exhibit. A high-availability setup for iSCSI is designed with the host running ISCSI software. Each storage port on the MDS exports the same two Fibre Channel target ports with different ISCSI target names. In this design, how many ISCSI session are created from the host so that recovery occurs if any component fails?

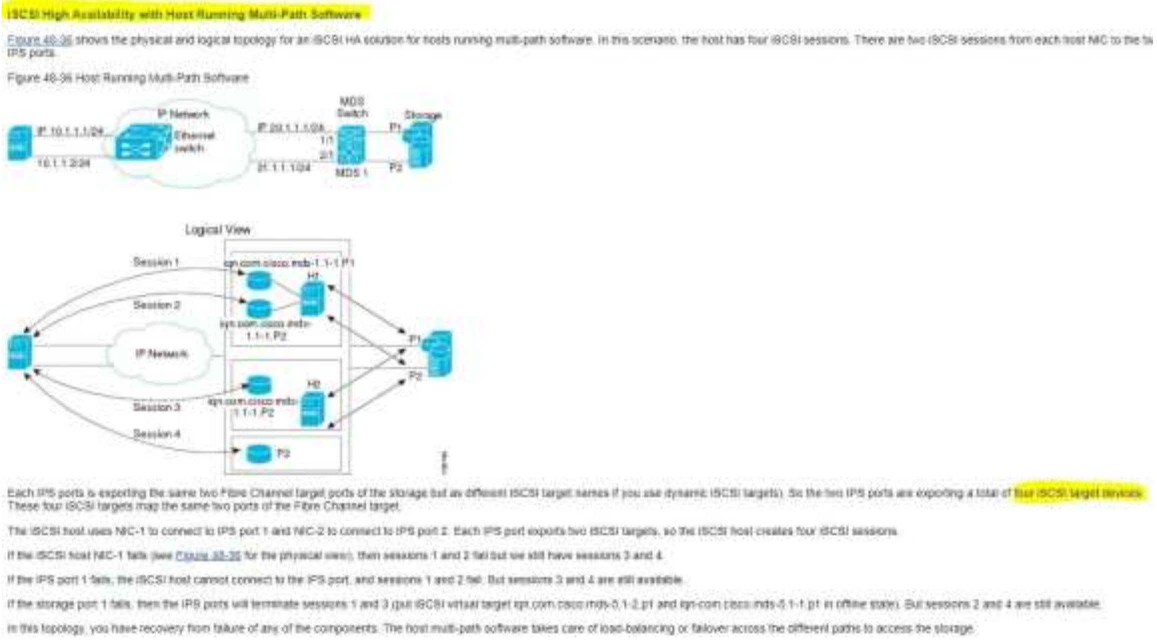


A. 2
B. 3
C. 4
D. 5

Answer: C

Explanation:

https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_3_x/configuration/guides/fm_3_2/ciscsi.html



iSCSI High Availability with Host Running Multi-Path Software

Figure 48-36 shows the physical and logical topology for an iSCSI HA solution for hosts running multi-path software. In this scenario, the host has four iSCSI sessions. There are two iSCSI sessions from each host NIC to the tw
IPS ports.

Figure 48-36 Host Running Multi-Path Software

Each IPS ports is exporting the same two Fibre Channel target ports of the storage but as different iSCSI target names if you use dynamic iSCSI targets). So the two IPS ports are exporting a total of four iSCSI target devices. These four iSCSI targets map the same two ports of the Fibre Channel target.

The iSCSI host uses NIC-1 to connect to IPS port 1 and NIC-2 to connect to IPS port 2. Each IPS port exports two iSCSI targets, so the iSCSI host creates four iSCSI sessions.

If the iSCSI host NIC-1 fails (see Figure 48-35 for the physical view), then sessions 1 and 2 fail but we still have sessions 3 and 4.

If the IPS port 1 fails, the iSCSI host cannot connect to the IPS port, and sessions 1 and 2 fail. But sessions 3 and 4 are still available.

If the storage port 1 fails, then the IPS ports will terminate sessions 1 and 3 (put iSCSI virtual target iqn.com.cisco.mds-5.1-2.p1 and iqn-com.cisco.mds-5.1-1.p1 in offline state). But sessions 2 and 4 are still available.

In this topology, you have recovery from failure of any of the components. The host multi-path software takes care of load-balancing or failover across the different paths to access the storage.

QUESTION 118
An engineer must design a Cisco UCS environment that will connection to a storage area network. The solution must include support for these conditions:
- connectivity to the existing 10 Gigabit Ethernet network
- booting the server infrastructure from the network
- integration with the existing Fibre Channel storage arrays
- lossless data transfer
Which solution should be used to meet these requirements?

A. FCP
B. FCoE
C. CIFS
D. NFS

Answer: B

QUESTION 119
An engineer requires a solution that achieves Ethernet traffic forwarding on all available paths from the hosts to the Cisco Nexus Fabric Extender and from the Fabric Extenders to the Cisco Nexus 5000 Series Switches. The NIC teaming from the Fabric Extender to a server should use an LACP EtherChannel. Which solution should be implemented to meet these requirements?

A. Virtual Port Channel
B. Enhanced Virtual Port Channel
C. Virtual Port Channel Plus (vPC+)
D. Back-to-Back Virtual Port Channel

Answer: B

QUESTION 120
A customer wants to deploy a Layer 2 extension over a transport infrastructure for multiple data centers. The data center technology should support a localized Layer 3 gateway, a separate flooding domain, and STP isolation per data center. Which DCI technology meets these requirements?

A. Pseudowire

B. VXLAN EVPN
C. E-Line
D. E-LAN

Answer: B

QUESTION 121
A network architect must design a large-scale Cisco SAN topology. The customer has a limited budget, so a design that provides use of resources is required. To support this requirement, the architect to share array ports, ISL, and line card bandwidth. The customer has also presented these additional considerations:
- The customers plans to expand the network by 10% over the next two years.
- The customer's policy requires physically separated infrastructure to support high availability.
Which solution should be used to meet these requirements?

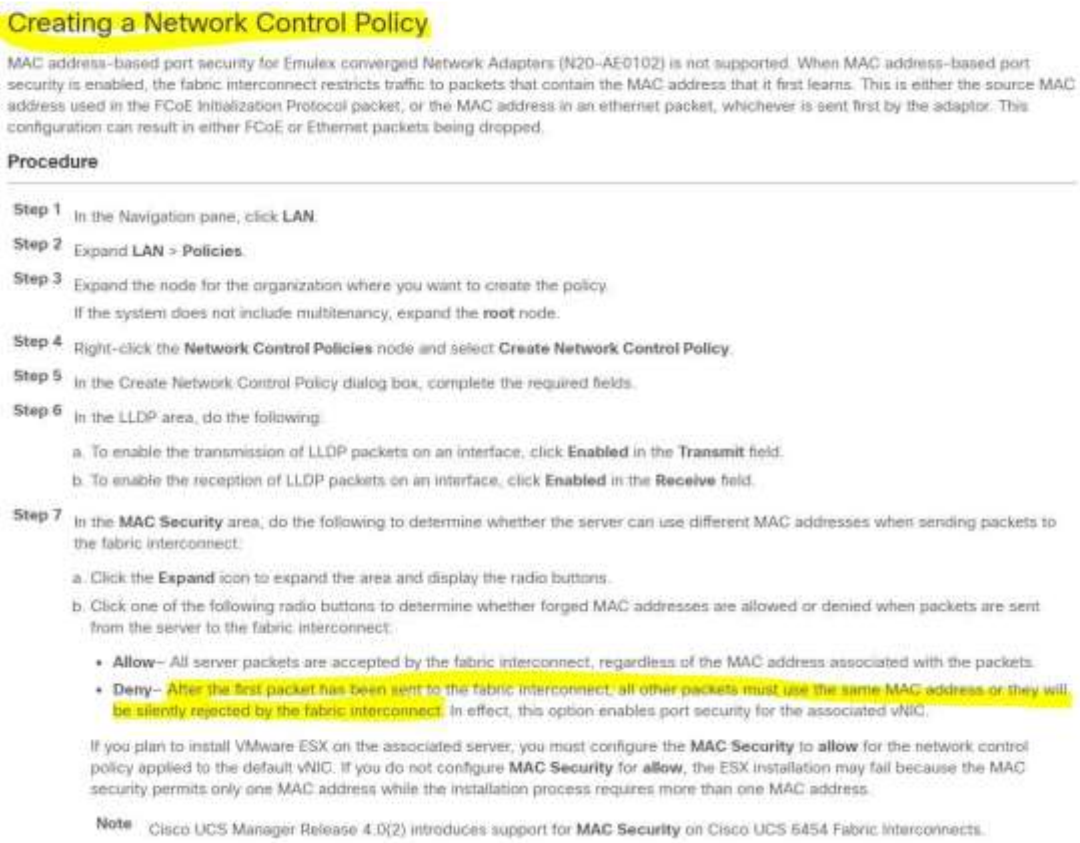
A. Collapsed-core
B. Mesh
C. Core-edge
D. Edge-core-edge

Answer: C

QUESTION 122
A company has several data centers with hundreds of Cisco UCS blade chassis. A network consultant plans to active Cisco Discovery Protocol to the servers to facilitate Layer 1 troubleshooting. For security reasons, the company wants to restrict the servers from sending different MAC addresses to the fabric interconnect after the MAC address from the first packet is learned. Which two policies be modified to support this design? (Choose two.)

A. Pin Group Policy
B. Network Control Policy
C. vNIC Policy
D. vNIC Template Policy
E. Ethernet Adapter

Answer: BD
Explanation:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/4-0/b_UCSM_Network_Mgmt_Guide_4_0/b_UCSM_Network_Mgmt_Guide_4_0_chapter_01010.html
https://jeremywaldrop.wordpress.com/2010/05/03/how-to-enable-cdp-on-cisco-ucs-vnics/



Creating a Network Control Policy

MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns. This is either the source MAC address used in the FCoE Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

Step 1 In the Navigation pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click the **Network Control Policies** node and select **Create Network Control Policy**.

Step 5 In the Create Network Control Policy dialog box, complete the required fields.

Step 6 In the LLDP area, do the following:

a. To enable the transmission of LLDP packets on an interface, click **Enabled** in the **Transmit** field.

b. To enable the reception of LLDP packets on an interface, click **Enabled** in the **Receive** field.

Step 7 In the **MAC Security** area, do the following to determine whether the server can use different MAC addresses when sending packets to the fabric interconnect:

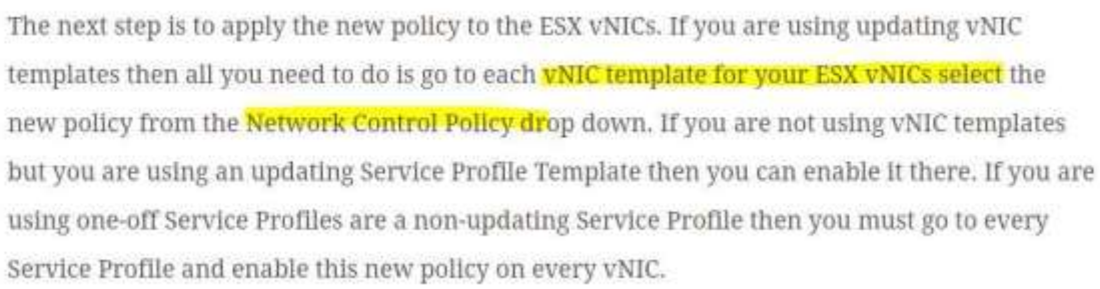
a. Click the **Expand** icon to expand the area and display the radio buttons.

b. Click one of the following radio buttons to determine whether forged MAC addresses are allowed or denied when packets are sent from the server to the fabric interconnect:

- **Allow**– All server packets are accepted by the fabric interconnect, regardless of the MAC address associated with the packets.
- **Deny**– After the first packet has been sent to the fabric interconnect, all other packets must use the same MAC address or they will be silently rejected by the fabric interconnect. In effect, this option enables port security for the associated vNIC.

If you plan to install VMware ESX on the associated server, you must configure the **MAC Security** to **allow** for the network control policy applied to the default vNIC. If you do not configure **MAC Security** for **allow**, the ESX installation may fail because the MAC security permits only one MAC address while the installation process requires more than one MAC address.

Note Cisco UCS Manager Release 4.0(2) introduces support for **MAC Security** on Cisco UCS 6454 Fabric Interconnects.



The next step is to apply the new policy to the ESX vNICs. If you are using updating vNIC templates then all you need to do is go to each vNIC template for your ESX vNICs select the new policy from the Network Control Policy drop down. If you are not using vNIC templates but you are using an updating Service Profile Template then you can enable it there. If you are using one-off Service Profiles are a non-updating Service Profile then you must go to every Service Profile and enable this new policy on every vNIC.

QUESTION 123
A customer asks an engineer to develop a framework to configure Cisco services that will be used to replace process of manual device configuration. The engineer plans to use a programmatic interface and must keep these considerations in mind:

```
- The customer's environment requires the script to authenticate before executing
further actions.
- The customer's security requirements mandate the use of HTTPS transport.
- The support stall has limited shell scripting knowledge, so the scripts should be easy
to read and write and be serf-documenting.
```

Which two solutions should be used to meet these requirements? (Choose two.)

A. Python scripts
B. REST calls
C. Bash scripts
D. domain-based policies
E. YAML

Answer: AB