

350-601^{Q&As}

Implementing and Operating Cisco Data Center Core Technologies
(DCCOR)

Pass Cisco 350-601 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/350-601.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

An engineer needs to monitor ingress traffic that arrives at interface Ethernet 1/3 that belongs to a Cisco Nexus 5600 Series Switch. The traffic analyzer machine located at interface Ethernet 1/5 is already monitoring other production, and the traffic analyzer must not be impacted by the traffic captured from the interface Eth1/3. The operations team allocated a traffic budget for the new monitoring session of 1 Gbps to meet this requirement.

Which set of commands configures the SPAN session?

- A.


```
interface Ethernet 1/3
monitor session 2
destination interface ethernet 1/5
source interface rx

interface Ethernet 1/5
monitor rate-limit 1G
```
- B.


```
interface Ethernet 1/3
monitor rate-limit 1G
destination interface ethernet 1/5
source interface rx

interface Ethernet 1/5
monitor session 2
destination interface tx
```
- C.


```
interface Ethernet 1/3
switchport monitor rate-limit 1G

monitor session 2
destination interface ethernet 1/5
source interface Eth 1/3
```
- D.


```
interface Ethernet 1/3 rx
switchport mode SD
switchport monitor rate-limit 1G
monitor session2
destination interface ethernet 1/5
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

Find Matches in This Book

	switch(config)# interface ethernet slot/port	Enters interface configuration mode for the specified Ethernet interface selected by the slot and port values.
Step 3	switch(config-if)# switchport monitor rate-limit 1G	Specifies that the rate limit is 1 Gbps.
Step 4	switch(config-if)# exit	Reverts to global configuration mode.

Example

This example shows how to limit the bandwidth on Ethernet interface 1/2 to 1 Gbps:

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport monitor rate-limit 1G
switch(config-if)#
```

Configuring Source Ports

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config) # monitor session session-number	Enters monitor configuration mode for the specified monitoring session.
Step 3	switch(config-monitor) # source interface type slot/port [rx tx both]	Adds an Ethernet SPAN source port and specifies the traffic direction in which to duplicate packets. You can enter a range of Ethernet, Fibre Channel, or virtual Fibre Channel ports. You can specify the traffic direction to duplicate as ingress (Rx), egress (Tx), or both. By default, the direction is both.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/system_management/7x/b_5600_System_Mgmt_Config_7x/configuring_span.html

QUESTION 2

DRAG DROP

An engineer is implementing security on the Cisco MDS 9000 switch.

Drag and drop the descriptions from the left onto the correct security features on the right.

Select and Place:

can be distributed via fabric services

uses the Exchange Fabric Membership Data protocol

allows a preconfigured set of Fibre Channel devices to logically connect to SAN ports

prevent unauthorized switches from joining the fabric or disrupting current fabric operations

Fabric Binding

Target 1

Target 2

Port Security

Target 3

Target 4

Correct Answer:

Fabric Binding

uses the Exchange Fabric Membership Data protocol

prevent unauthorized switches from joining the fabric or disrupting current fabric operations

Port Security

can be distributed via fabric services

allows a preconfigured set of Fibre Channel devices to logically connect to SAN ports

Fabric Binding:

- Uses the Exchange Fabric Membership Data Protocol
- Prevent unauthorized switches from joining the fabric or disrupting current fabric operations

Port Security:

- Can be distributed via fabric services
- Allows a preconfigured set of Fibre Channel devices to logically connect to a SAN ports.

Reference: https://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/san_switching/7x/b_5500_SAN_Switching_Config_7x_chapter_010010.html#con_1170967

QUESTION 3

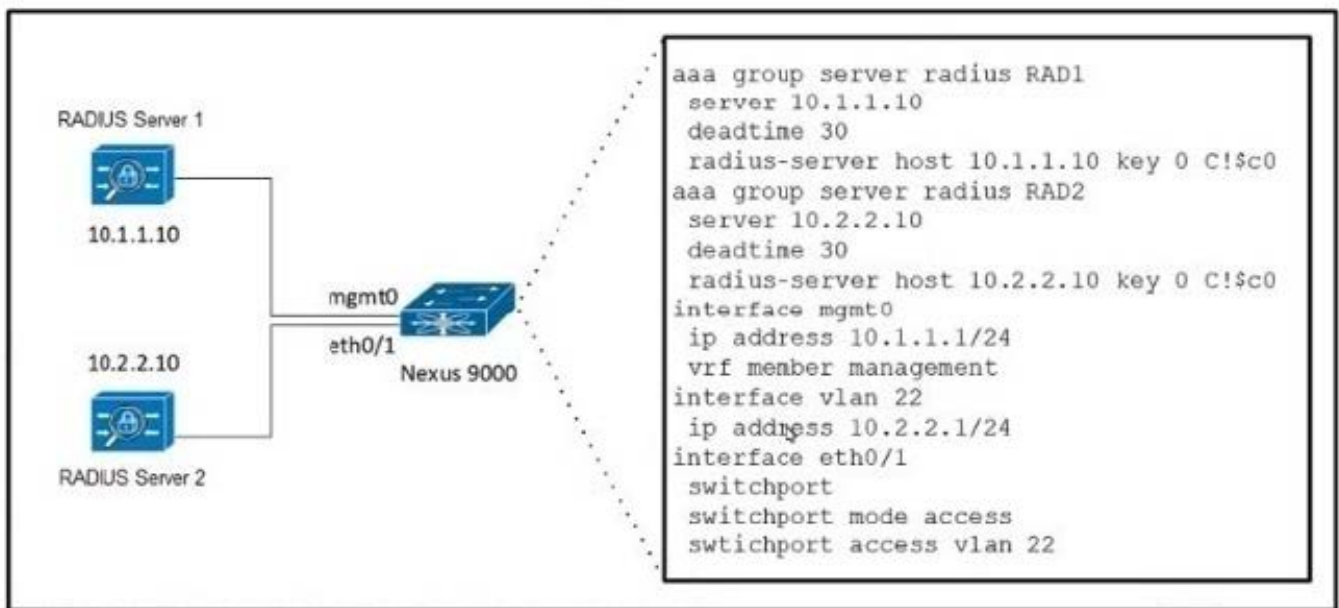
Which two statements describe the process of upgrading an EPLD on a Cisco MDS 9000 Series Switch? (Choose two.)

- A. EPLDs are only capable to be upgraded to the latest EPLD image.
- B. EPLD upgrades are capable to be completed without powering down the module during the upgrade.
- C. An upgrade verification identifies the impact of each EPLD upgrade.
- D. The EPLDs for all the modules on a switch must be upgraded at the same time.
- E. EPLDs are capable to be upgraded without replacing the hardware.

Correct Answer: CE

QUESTION 4

Refer to the exhibit.



A user must be granted management access to the Cisco Nexus 9000 Series Switch using AAA servers. The RADIUS servers are configured to accept login requests from the same Layer 2 subnet of the switch. The user must be permitted to log in with these requirements:

1.
RADIUS server 1 must be used to log in via a console.
2.
RADIUS server 2 must be used to log in via SSH.

Which two actions meet these requirements?

- A. Enable command authorization to RAD1 and RAD2 for all successful logins.
- B. Change the dead timer for RAD1 and RAD2 to 1 minute.
- C. Set the RADIUS source interface to be mgmt0 for group RAD1 and VLAN 22 for group RAD2
- D. Configure the authentication login to use group RAD1 for console and group RAD2 for remote access.

Correct Answer: AD

QUESTION 5

Which value is missing in the field in the key called "msg" in this JSON response?

Request:

```
{
  "ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "sid": "1",
    "input": "show switchname",
    "output_format": "json"
  }
}
```

Response:

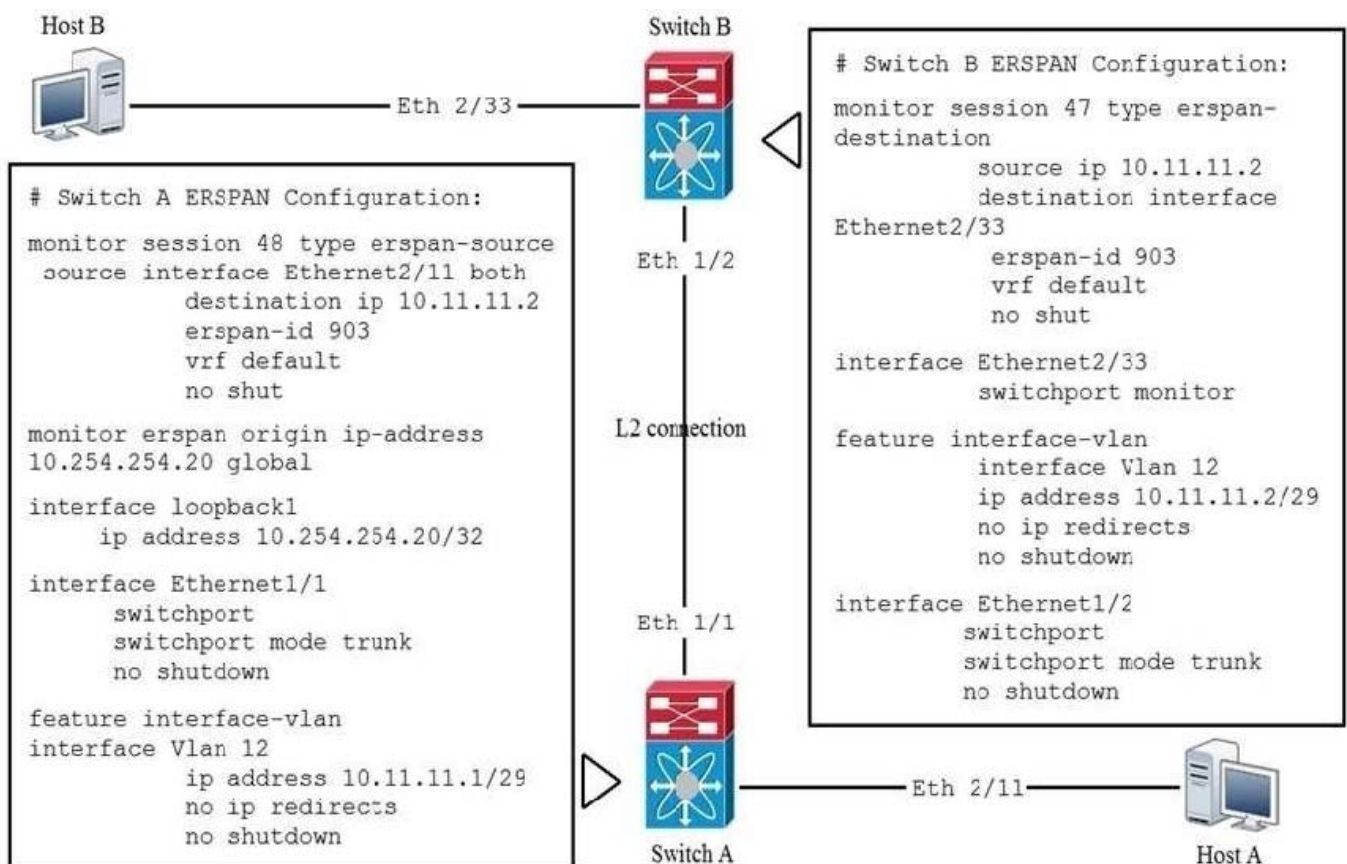
```
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show switchname",
        "msg": "<missing_value>",
        "code": "200",
        "body": {
          "hostname": "switch456336289237"
        }
      }
    }
  }
}
```


- A. Success
- B. Available
- C. Unavailable
- D. Drop

Correct Answer: A

QUESTION 6

Refer to the exhibit.



Which statement about the ERSPAN configuration in this environment is true?

- A. Host A is the source of ERSPAN spanned traffic and host B is the traffic analyzer.
- B. Host B is the source of ERSPAN spanned traffic and host A is the traffic analyzer.
- C. The session number of the source of ERSPAN spanned traffic must have a session ID of 48 for the traffic analyzer to receive the traffic.
- D. The session number of the source of ERSPAN spanned traffic must have a session ID of 47 for the traffic analyzer to

receive the traffic.

Correct Answer: A

QUESTION 7

A network administrator must perform a system upgrade on a Cisco MDS 9000 Series Switch. Due to the recent changes by the security team:

1.

The AAA server is unreachable.

2.

All TCP communication between the MDS 9000 Series Switch and AAA servers is disabled. Which actions must be used to perform the upgrade?

A. Log in locally to the MDS 9000 Series Switch using a network-admin role and download the upgrade files from the remote TFTP server.

B. Log in locally to the MDS 9000 Series Switch using a server-admin role and download the upgrade files from the remote FTP server.

C. Log in to a server storing the upgrade files remotely using a server-admin role and download the files to the MDS 9000 Series Switch using SFTP.

D. Log in to a server storing the upgrade files remotely using a network-admin role and download the files to the MDS 9000 Series Switch using HTTP.

Correct Answer: A

Of all the answer choices, only TFTP does not use TCP. TFTP is a UDP based protocol.

QUESTION 8

An engineer must perform a configuration backup of an existing Cisco UCS Manager environment. The backup file must contain all vNIC, vHBA, and service profile template settings. Also, the engineer must validate the backup before import and requires an XML output format. Which backup type must be used to meet these requirements?

A. full state

B. all configuration

C. logical configuration

D. system configuration

Correct Answer: C

QUESTION 9

An engineer must configure a Cisco MDS 9000 Series Switch for traffic analysis from the storage array. The storage array is connected to the interface fc2/1 in VSAN 10 and the traffic analyzer to fc4/2. The capture file must include ingress and egress traffic between the switch and the storage array. Also, only traffic in VSAN 10 must be captured.

Which configuration set meets these requirements?

A. interface fc4/2 switchport mode trunk switchport trunk allow vsan 10 no shutdown ! span session 1 source interface fc2/1 tx destination interface fc4/2 rx no suspend

B. interface fc4/2 switchport mode SD no shutdown ! span session 1 source interface fc2/1 destination interface fc4/2 source filter vsan 10

C. interface fc4/2 switchport mode auto no shutdown ! span session 1 source interface fc2/1 rx destination interface fc4/2 source filter vsan 10 no suspend

D. interface fc4/2 switchport mode ST no shutdown ! span session 1 source interface fc2/1 destination interface fc4/2 source filter vsan 10

Correct Answer: B

QUESTION 10

Refer to the exhibit. An engineer is configuring Cisco Data Center Network Manager to automate the provisioning of Cisco Nexus 9000 Series Switches. The engineer must configure user access for network engineers to permit device operations in Interface Manager. The solution must hide Admin and Config Menu items in Interface Manager. Which two roles must be assigned to the network engineers to meet these requirements? (Choose two.)

The table below lists the roles supported by Cisco DCNM:

Role	Description
global-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate LAN and SAN features.
network-admin	General role to administrate LAN features.
lan-network-admin	General role to administrate LAN features.
san-network-admin	General role to administrate SAN features.
san-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate SAN features.
server-admin	Introduced in the FlexAttach feature, a role that administrates FC server host feature.
sme-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME feature.
sme-stg-admin	Introduced in the Storage Media Encryption (SME)) feature, a role that administrates SME storage.
sme-kmc-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME Key Management.
sme-recovery	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME recovery.
network-operator	General network operator role.
device-upg-admin	This role is added to perform operations only in Image Management window.
access-admin	This role is introduced to perform operations in Interface Manager window for all fabrics.

Table 2: DCNM Roles and Perspectives Mapping Table

Role	Perspective
global-admin	Admin Perspective
network-admin	
san-admin	
san-network-admin	
lan-network-admin (Web Client)	
server-admin	Server Admin Perspective
sme-admin	SME Perspective
sme-sgt-admin	
sme-kmc-admin	
sme-recovery	
network-operator	Operator Perspective
lan-network-admin (SAN Client)	
access-admin	
device-upg-admin	

- A. network-admin
- B. global-admin
- C. access-admin
- D. network-operator
- E. san-admin

Correct Answer: CD

QUESTION 11

Refer to the exhibit.

```
ACI-Leaf1# show ip route vrf DATACENTER:DC
10.20.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.8.65%overlay-1, [1/0], 4w3d, static
172.16.100.0/24, ubest/mbest: 1/0
    *via 10.1.168.95%overlay-1, [200/5], 3w0d, bgp-132, internal, tag 132 (mpls-vpn)
172.16.99.0/24, ubest/mbest: 1/0
    *via 10.0.1.14, [20/0], 3w0d, bgp-132, external, tag 200
```

Which two statements describe the routing table of the leaf switch? (Choose two.)

- A. The next hop 10.0.8.65 for route 10.20.1.0/24 is the TEP address of a border leaf in ACI.
- B. The next hop 10.0.1.14 for route 172.16.99.0/24 is the TEP address of a border leaf in ACI.
- C. The next hop 10.1.168.95 for route 172.16.100.0/24 is the TEP address of a border leaf in ACI.
- D. 172.16.100.0/24 is a BD subnet in ACI.
- E. 10.20.1.0/24 is a BD subnet in ACI.

Correct Answer: CE

QUESTION 12

Port security is enabled on a Cisco MDS 9000 series Switch. Which statement is true?

- A. Cisco Fabric Services must be disabled before enabling port security.
- B. Port security can be enabled only globally and affects all VSANs.

C. Auto-learning is always enabled automatically when port security is enabled.

D. Any devices currently logged in must be added manually to the device databased.

Correct Answer: C

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_port_security.html

- **Active database** The database currently enforced by the fabric. The port security feature requires all devices connecting to a switch to be part of the port security active database. The software uses this active database to enforce authorization.

About Auto-Learning

You can instruct the switch to automatically learn (auto-learn) the port security configurations over a specified period. This feature allows any switch in the Cisco MDS 9000 Family to automatically learn about devices and switches that connect to it. Use this feature when you activate the port security feature for the first time as it saves tedious manual configuration for each port. You must configure auto-learning on a per-VSAN basis. If enabled, devices and switches that are allowed to connect to the switch are automatically learned, even if you have not configured any port access.

When auto-learning is enabled, learning happens for the devices or interfaces that were already logged into the switch and the new devices or interfaces that need to be logged in. Learned entries on a port are cleaned up after you shut down that port if auto-learning is still enabled.

Learning does not override the existing configured port security policies. So, for example, if an interface is configured to allow a specific pWWN, then auto-learning will not add a new entry to allow any other pWWN on that interface. All other pWWNs will be blocked even in auto-learning mode.

No entries are learned for a port in the shutdown state.

When you activate the port security feature, auto-learning is also automatically enabled.



Note

If you activate port security feature, auto-learning gets enabled by default. You cannot re-activate port security until auto-learning is disabled or deactivate and activate again.

Port Security Activation

By default, the port security feature is not activated in any switch in the Cisco MDS 9000 Family.

By activating the port security feature, the following apply:

- Auto-learning is also automatically enabled, which means:
 - From this point, auto-learning happens for the devices or interfaces that were already logged into the switch and also for the new devices will login in future.
 - You cannot activate the database until you disable auto-learning.
- All the devices that are already logged in are learned and are added to the active database.
- All entries in the configured database are copied to the active database.

After the database is activated, subsequent device login is subject to the activated port bound WWN pairs, excluding the auto-learned entries. You must disable auto-learning before the auto-learned entries become activated.

When you activate the port security feature, auto-learning is also automatically enabled. You can choose to activate the port security feature and disable auto-learning.

QUESTION 13

An engineer must perform an initial configuration of VXLAN Tunnel End-Point functionality on the Cisco Nexus 9000

Series platform. All the necessary features are already enabled on the switch. Which configuration set must be used to accomplish this goal?

- A. NX9K(config)# interface loopback0 NX9K(config-if)# ip address 10.10.10.11/32 NX9K(config)# interface VLAN10 NX9K(config-if)# ip unnumbered loopback0 NX9K(config)# interface nve1 NX9K(config-if-nve)# source-interface loopback0
- B. NX9K(config)# interface loopback0 NX9K(config-if)# ip address 10.10.10.11/32 NX9K(config)# interface overlay0 NX9K(config-if-overlay)# source-interface loopback0 NX9K(config)# interface VLAN10 NX9K(config-if-nve)# source-interface loopback0
- C. NX9K(config)# interface loopback0 NX9K(config-if)# ip address 10.10.10.11/32 NX9K(config)# interface tunnel1 NX9K(config-if)# tunnel source loopback0 NX9K(config)# interface ethernet1/1 NX9K(config-if)# ip unnumbered loopback0
- D. NX9K(config)# interface loopback0 NX9K(config-if)# ip address 10.10.10.11/32 NX9K(config)# interface nve1 NX9K(config-if-nve)# source-interface loopback0 NX9K(config)# interface ethernet1/1 NX9K(config-if)# ip unnumbered loopback0

Correct Answer: D

QUESTION 14

An engineer must configure a Cisco UCS blade system that is managed by Cisco UCS Manager. All four connected interfaces between the blade system and the fabric interconnects must be used. Additionally, the connectivity must tolerate any link failure between the I/O module and the fabric interconnects. Which action accomplishes these requirements?

- A. Configure port aggregation with LACP policy set to default
- B. Configure Firmware Auto Sync Server policy to Auto Acknowledge
- C. Configure Link Group Preference to Port Channel.
- D. Configure chassis/FEX discovery pokey action to four links

Correct Answer: C

QUESTION 15

Cisco Nexus 9000 Series Switches are configured with LACP protocol and default aging timers. What is the impact on the LACP peer during an ISSU upgrade?

- A. The LACP peer connection terminates.
- B. The LACP peer session remains up.
- C. The LACP peer renegotiates the adjacency.
- D. The LACP peer connection resets.

Correct Answer: B

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/interfaces/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Interfaces_Configuration_Guide/b_Cisco_Nexus_9000_Series_NXOS_Interfaces_Configuration_Guide_chapter_0110.html ISSU and ungraceful switchovers are not supported with LACP fast timers.

[350-601 PDF Dumps](#)

[350-601 VCE Dumps](#)

[350-601 Practice Test](#)