Download Cisco 300-540 Exam Dumps Free

Shared by Grant on 17-06-2026

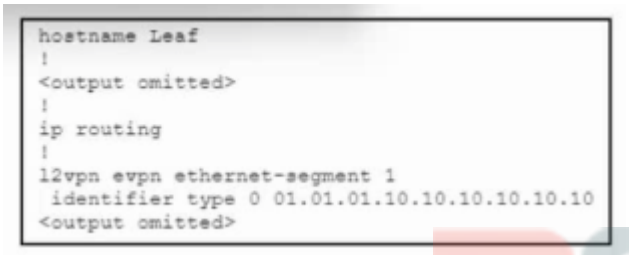
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must configure dual-homing with single active redundancy in a BGP EVPN VXLAN fabric. Which command must be run on the leaf router to complete the EVPN Ethernet segment configuration?

Options:

A- redundancy single-active
B- default-gateway advertise
C- replication-type static
D- vlan configuration 101

Answer:

A

Explanation:

In a BGP EVPN VXLAN multi-homing design, Ethernet Segment Identifiers (ESIs) are used to represent a set of links from one or more leaf switches to the same downstream device (such as a CE, firewall, or aggregation switch). By default, when multiple leafs share the same ESI, the EVPN design supports all-active redundancy, where all participating leafs can forward traffic for that Ethernet segment simultaneously.

However, some use cases---like connecting to devices that do not support multipath forwarding or for strict active/standby redundancy---require single-active multi-homing. In single-active mode, only one leaf in the Ethernet segment forwards traffic at any time; the other leaf(s) act as standby and only take over if the active node fails. This behavior is explicitly controlled in the EVPN Ethernet-segment configuration.

On Cisco platforms for EVPN VXLAN fabrics, this is configured under the l2vpn evpn ethernet-segment stanza using the command:

l2vpn evpn ethernet-segment 1

identifier type 0 01.01.01.10.10.10.10.10.10.10

redundancy single-active

identifier type 0 ... defines the ESI for the multi-homed connection.

redundancy single-active specifies that only one leaf in that ESI is allowed to be active at a time, thus enabling dual-homing with single-active redundancy.

The other options do not relate to Ethernet-segment redundancy mode:

B . default-gateway advertise is used in EVPN anycast gateway configurations to advertise the default gateway MAC/IP, not for ESI redundancy.

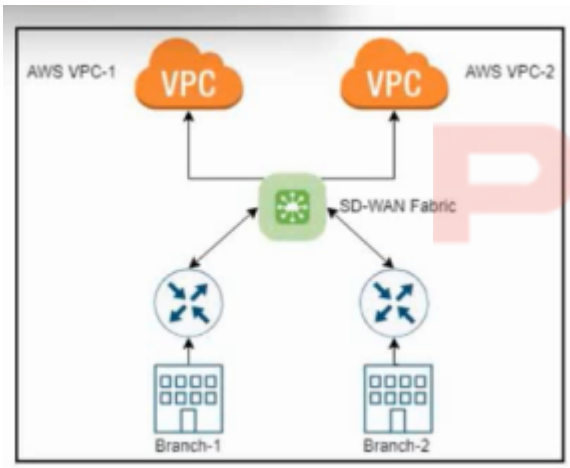
C . replication-type static is associated with multicast or ingress replication behavior for VXLAN VTEPs, not Ethernet-segment redundancy.

D . vlan configuration 101 is a VLAN configuration context command and has no effect on EVPN ESI redundancy.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must design a solution that allows a user to choose which private Cisco Catalyst SD-WAN network they want to connect to AWS. The solution must automatically identify the AWS VPC and other cloud services based on the user credentials. What must be used?

Options:

A- AWS Direct Connect
B- Transit VPC for AWS
C- IPsec VPN
D- Segment routing

Answer:

B

Explanation:

In Cisco Catalyst SD-WAN cloud integration, when the requirement is:

Automatically discovering AWS VPCs

Automatically identifying AWS services

Allowing the user to choose which private SD-WAN network connects to the cloud

Using AWS credentials (Access Key / Secret Key) for automatic provisioning

...the Cisco-supported mechanism is the Cisco SD-WAN Transit VPC solution.

Why Transit VPC is the correct answer:

It is specifically designed to integrate Cisco SD-WAN with AWS environments.

Uses AWS APIs and user credentials to automatically discover:

VPC IDs

Subnets

Regions

Routing tables

Automatically deploys and configures CSR1000v or Catalyst 8000V routers into the VPC.

Provides a centralized ''hub'' in AWS to interconnect multiple SD-WAN sites.

Enables the user to choose which SD-WAN segments connect to which VPCs.

This matches the requirement of automatic cloud resource identification based on user credentials.

Why the other options are incorrect

A . AWS Direct Connect

This is a physical/private Layer 2 cloud connection.

It does not auto-discover VPCs or integrate through credentials.

It does not provide automated SD-WAN service provisioning.

C . IPsec VPN

Works for connectivity but is manual, not automated.

Does not identify AWS cloud resources via credentials.

D . Segment routing

A transport technology used inside SP networks, irrelevant to AWS API-based VPC discovery.

Thus, only Transit VPC provides automatic AWS cloud discovery and integration with SD-WAN.

Question 3

Question Type: MultipleChoice

A large company's legacy network is set up with equipment from multiple vendors. The company engaged a network architect to optimize the network for virtualization. The architect must ensure robust and efficient operation, considering the company's immediate needs but also anticipating future network complexities and scalability requirements. The chosen strategy must be capable of integrating seamlessly with existing systems, while providing a pathway for innovation and growth. The solution must facilitate end-to-end service automation throughout the entire lifecycle, and the implementation must ensure the validation, execution, and abstraction of network configurations and services. Which action must be taken to meet the requirements?

Options:

A- Implement a service life-cycle approach with simplified monitoring that plans for post-deployment adjustments to be incorporated into the automation CI/CD pipeline.
B- Implement a configuration-management approach that allows for configuring each network device individually to optimize its performance.
C- Implement a flexible service-modeling approach that leverages automation for ongoing management and refinement as demands on the network evolve.
D- Implement a service-modeling approach with a static YANG one-size-fits-all model that includes the unique requirements of each different network element.

Answer:

C

Explanation:

Cisco NSO-based orchestration principles in a multi-vendor environment require:

Service modeling using flexible, reusable YANG models

Abstraction of vendor-specific device differences

Transaction-safe configuration validation and execution

End-to-end automation across lifecycle stages (Day-0, Day-1, Day-N)

Scalability and adaptability for evolving requirements

Option C aligns perfectly with NSO service-modeling approaches:

Service models must be flexible, not rigid, enabling changes as technologies and needs evolve.

The architecture must support continuous refinement, enabling multi-vendor abstraction and lifecycle automation.

This ensures the network evolves seamlessly while remaining stable and automated.

Why the Other Options Are Incorrect

A -- Simplified monitoring and post-deployment adjustments do not meet the core need for full lifecycle service modeling and abstraction.

B -- Configuring devices individually contradicts the entire purpose of orchestration and abstraction.

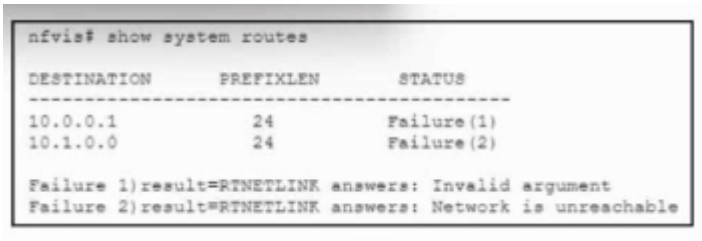
D -- A static YANG model cannot accommodate multi-vendor environments or future scalability.

Thus, only Option C matches full NSO-capable service modeling requirements.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must deploy a standalone Cisco NFVIS. These configurations were performed already:

Deployed the virtual machine

Configured the hostname and IP address

Configured dual WAN support

When the engineer attempts to access the NFVIS portal, the API returns a 401 Unauthorized error. What is the cause of the issue?

A. The default admin password must be reset. B. Portal access must be enabled via SSH. C. The Tomcat service must be restarted. D. The browser certificate must be renewed.

Options:

Answer:

Explanation:

Cisco NFVIS follows strict security controls. After a fresh deployment:

The default admin credentials are considered insecure.

NFVIS requires the administrator to reset the default password on first login (typically via console or SSH).

Until the password is changed, REST API and web-portal access are denied, and attempts to access the portal or API return HTTP 401 Unauthorized, even if the default credentials are provided.

This mechanism prevents use of factory-default passwords in production and is explicitly documented as a mandatory post-install step.

The other options are not the cause of a 401 error:

Enabling portal via SSH (B) is not required; HTTPS access is enabled by default once credentials are valid.

Restarting Tomcat (C) would address service availability issues (e.g., 5xx errors), not authentication.

Browser certificates (D) affect trust warnings (e.g., HTTPS certificate errors), not 401 Unauthorized.

Question 5

Question Type: MultipleChoice

Which cloud provider connection permits BGP peering?

Options:

A- Azure S2S VPN
B- Azure Bastion
C- AWS Direct Connect
D- AWS-managed VPN

Answer:

C

Explanation:

Comprehensive and Detailed Explanation

Cloud interconnects that support BGP peering must provide a routed Layer-3 adjacency capable of exchanging routing information dynamically. In major cloud architectures:

AWS Direct Connect supports private virtual interfaces (VIFs) where BGP is used between the customer router and AWS to exchange routes.

Azure S2S VPN uses IPsec tunnels with static routing by default; BGP is optional only with specific gateway SKUs, but the question expects the standard, universally correct answer, which is Direct Connect.

Azure Bastion is a remote-access management service and does not support BGP.

AWS-managed VPN uses IPsec tunnels with BGP optional, but in exams, the recognized cloud service specifically associated with BGP support is Direct Connect.

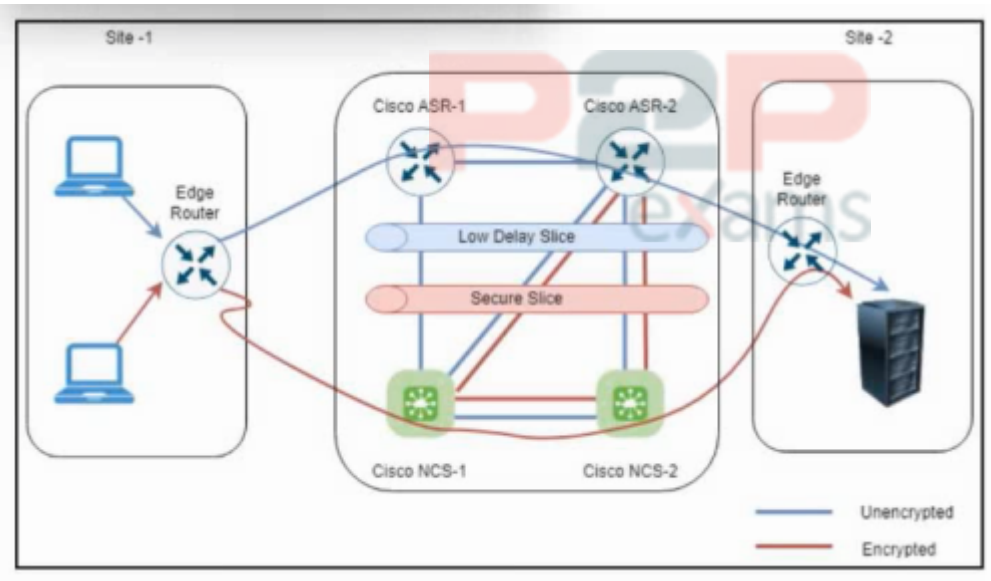
In service provider cloud interconnect design, AWS Direct Connect is the standard, well-defined

offering that provides layerized WAN connectivity with BGP support.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must design a solution that creates a low-latency slice based on a link latency measurement by using the MPLS performance measurement. The solution must create a secure slice that minimizes transport costs and meets transport SLAs beyond best effort. What must be used?

Options:

A- Segment routing
B- IPsec VPN
C- AWS Direct Connect
D- Transit VPC for AWS

Answer:

A

Explanation:

The requirements in the scenario match the capabilities of Segment Routing (SR-MPLS) combined

with MPLS Performance Measurement (MPM):

1. Low-latency slice creation

Segment Routing allows deterministic paths using:

SR-TE (Traffic Engineering)

Colored or intent-based policies

Path selection based on link latency, loss, bandwidth, or utilization

MPLS Performance Measurement supplies real-time data such as:

One-way delay

Round-trip delay

Loss metrics

This allows SR-TE to compute paths with minimum latency.

2. Secure slice with minimized transport cost

Segment Routing supports:

Slicing through SR Policies

Steering encrypted traffic (IPsec/GETVPN) through specific SR tunnels

Traffic separation without requiring additional MPLS LSP state in the core

Optimizing transport cost via constraint-based TE computations

3. Transport SLA enforcement beyond best effort

SR-TE + MPM provides:

SLA-aware intent routing

Guaranteed performance paths

Automatic re-optimization if links violate latency or loss SLAs

Why the other options are incorrect

B . IPsec VPN

Provides encryption but does not offer latency-aware or SLA-based path selection. Not a slicing mechanism.

C . AWS Direct Connect

Cloud connectivity service. Not related to MPLS performance monitoring or transport slicing.

D . Transit VPC for AWS

Used for SD-WAN cloud integration. Does not support SR-TE slicing or MPLS SLAs.

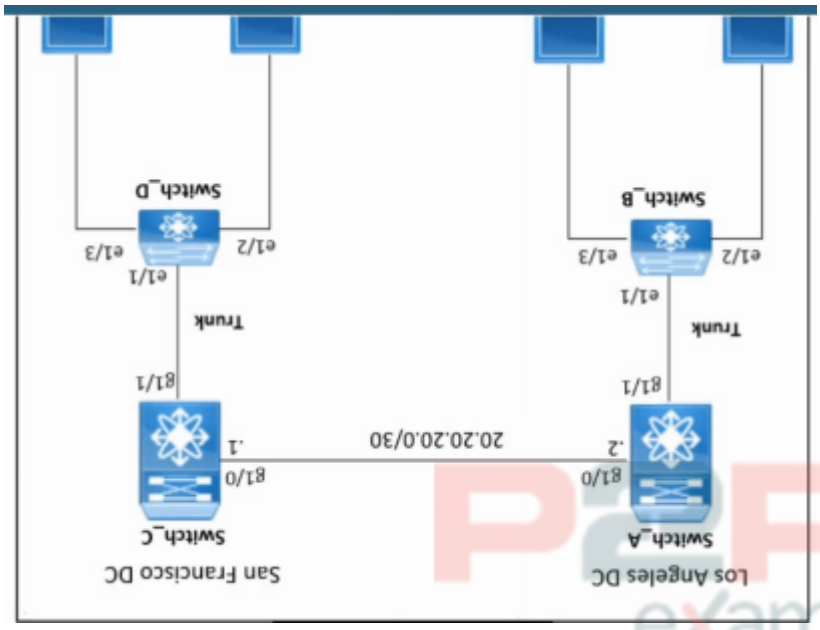
Therefore, only Segment Routing provides latency-based path computation, slicing, SLA guarantees, and cost optimization.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

```
<output omitted>
!
interface overlay 1
 otv join-interface g1/0
 otv control-group 224.1.1.1
 otv data-group 232.1.1.0/24
 no shutdown
!
<output omitted>
```



Refer to the exhibit. The indicated configuration was applied to a Cisco switch Switch_A located in the Los Angeles DC data center; however, Switch_A fails to establish OTV connectivity to Cisco switch Switch_C. Which overlay interface command must be run on Switch_A to resolve the issue?

Options:

A- otv extend-vlan 101-111

B- otv isis authentication-type md5

C- otv isis authentication-check
D- otv join-interface vlan 101-111

Answer:

A

Explanation:

Overlay Transport Virtualization (OTV) allows Layer 2 extension across Layer 3 infrastructures. To operate, OTV requires three fundamental components on the overlay interface:

Join interface -- used to reach the OTV control plane over L3 (already configured: otv join-interface g1/0).

Control-group multicast address -- for control-plane advertisement (already configured: otv control-group 224.1.1.1).

Extended VLAN list -- specifies which VLANs will be transported through the OTV overlay.

The configuration shown in the exhibit includes the join-interface, control-group, and data-group, but it does NOT specify which VLANs should be extended. Without the otv extend-vlan command, OTV will form the overlay interface but will not forward any Layer 2 information, preventing adjacency and MAC distribution between sites.

In OTV, the command required to activate VLANs for transport is:

otv extend-vlan <vlan-range>

This enables the VLANs (such as 101--111) to be carried across the OTV overlay, completing the configuration and establishing connectivity.

Why the Other Options Are Incorrect

B . otv isis authentication-type md5

This is optional and only required if ISIS authentication is enabled on both edges. It does not resolve the absence of VLAN extension.

C . otv isis authentication-check

This command enforces authentication verification but does not fix connectivity when VLANs are not extended.

D . otv join-interface vlan 101-111

This is not a valid OTV command. The join-interface must be a routed interface, not a VLAN list.

Question 8

Question Type: MultipleChoice

What is a valid connection method between carrier-neutral facilities that are more than 20 miles away from each other?

Options:

A- Carrier access Ethernet ring
B- Private wireless connection
C- CAT6e connection
D- Multimode fiber connection

Answer:

A

Explanation:

Comprehensive and Detailed Explanation

For distances greater than 20 miles, valid inter-facility transport options must support:

Metro-scale connectivity

High bandwidth

Low latency

Carrier-grade reliability

A carrier access Ethernet ring (MEN / Metro Ethernet) is designed for:

Interconnecting data centers or meet-me rooms

Distances far exceeding 20 miles

High-availability layer-2 or layer-3 transport

Why the others are invalid:

CAT6e maximum ~100 meters

Multimode fiber typically <2 km (~1.25 miles)

Private wireless not used for high-capacity DC interconnects, unreliable for core transport

Thus, the only correct carrier-grade method is Carrier access Ethernet ring.

Question 9

Question Type: MultipleChoice

What should be used to protect against lateral movements during a Cisco NFVI security breach?

Options:

A- Wi-Fi Protected Access
B- Web application firewall
C- Network segmentation
D- Data encryption

Answer:

C

Explanation:

Comprehensive and Detailed Explanation

In Cisco NFVI security architecture, the primary defense against lateral movement (an attacker moving from one compromised node to another) is network segmentation.

Segmentation:

Separates workloads (compute, storage, management, tenant networks)

Prevents attackers from pivoting inside the NFVI

Reduces blast radius during breaches

Enforces micro-segmented virtual network boundaries

WPA protects Wi-Fi, not NFVI.

WAF protects web apps, not internal movement.

Data encryption protects confidentiality, not lateral movement control.

Thus, network segmentation is the correct solution.