PassQueen
a.k.a dumpsqueen.com

Cisco Application Centric Infrastructure for Field Engineers Exam

Cisco 700-703

Version Demo

Total Demo Questions: 9

Total Premium Questions: 90

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, ACI Fabric Components	43
Topic 2, ACI Fabric Setup	4
Topic 3, ACI Fabric Configuration	37
Topic 4, ACI Fabric Operations	6
Total	90

QUESTION NO: 1

Where in the APIC GUI are Layer 2 and Layer 3 networks created?

A. VM Networking > inventory

B. Fabric > Access policies

C. VM networking > policies

D. Tenants > Tenant_Name > Networking

ANSWER: D

Explanation:

Layer 2 and Layer 3 tenant networks are created under **Tenants > Tenant_Name > Networking** in the APIC GUI. ACI uses a tenant-based logical model: networking constructs that define tenant connectivity belong to the tenant configuration rather than to fabric access configuration. From the selected tenant's Networking area, an administrator creates and manages objects such as VRFs, bridge domains, subnets, and external routed networks. A bridge domain provides the Layer 2 forwarding scope and is associated with a VRF to provide the Layer 3 routing context. Tenant subnets define the Layer 3 gateway addresses associated with bridge domains, while Layer 3 outside connectivity is configured as an L3Out within the tenant. This placement lets APIC maintain isolation and policy boundaries between tenants while associating endpoint groups and contracts with the appropriate forwarding configuration. Cisco's APIC configuration documentation describes bridge domains, VRFs, and external Layer 3 connectivity as tenant networking objects, and Cisco's ACI API documentation likewise models these objects within tenant configuration. See the Cisco APIC Basic Configuration Guide and Cisco ACI object model documentation.

QUESTION NO: 2

Which two new operational models are driving the need for infrastructure change in business today? (Choose two.)

A. Big data

B. Increased time to market

C. Increased data center costs

D. Cloud computing

E. Increasing IT staff

ANSWER: A D

Explanation:

Big data and cloud computing are the operational models driving the need to evolve data-center infrastructure. Big-data workloads involve high volumes, velocity, and variety of data, often requiring distributed compute and storage resources as well as scalable, predictable network connectivity between applications, analytics platforms, and data repositories. This demand makes static, manually managed infrastructure less suitable for modern application environments.

Cloud computing similarly changes how infrastructure is consumed and operated. Cloud models emphasize on-demand access, rapid provisioning, resource pooling, elasticity, automation, and service-oriented delivery. To support these expectations, the network must be programmable and policy-driven so that application connectivity, security requirements, and segmentation can be deployed consistently at cloud-like speed. Cisco ACI is designed around this application-centric, policy-based approach to data-center networking, helping infrastructure teams align network operations with dynamic application and cloud consumption models. Cisco discusses the need for automated, policy-driven data-center infrastructure in its Application Centric Infrastructure overview. The operational characteristics of cloud computing are also defined by NIST in its cloud-computing definition.

QUESTION NO: 3

In an application-centric infrastructure which four aspects of the solution must be configured to support an application? (Choose four.)

A. The relationship between endpoints and their policies.

B. Data center-specific configuration of the infrastructure.

C. The endpoints of the application.

D. The layer 2 through layer 7 network policies of the application.

E. A virtual machine or server

F. Establishes forwarding paths in the ACI fabric.

ANSWER: A B C D

Explanation:

An application-centric infrastructure requires configuration that expresses both the application's connectivity intent and the fabric context in which that intent is enforced. **The endpoints of the application** must be identified and classified, typically through endpoint groups, so that the fabric can apply consistent connectivity and security treatment as workloads attach or move. **The relationship between endpoints and their policies** is required because ACI associates endpoint groups with the policy constructs governing allowed communications. **The layer 2 through layer 7 network policies of the application** define the application connectivity requirements, including forwarding and segmentation behavior as well as service insertion where needed. These policies are represented through ACI constructs such as bridge domains, VRFs, contracts, filters, and service graphs. **Data center-specific configuration of the infrastructure** supplies the fabric-side prerequisites for deploying that policy, including access connectivity and integration with the particular data-center environment. Together, these elements allow APIC to translate application intent into policy enforcement throughout the ACI fabric. Cisco describes ACI as a policy-driven architecture that uses application profiles, endpoint groups, and contracts to define application connectivity: Cisco Application Centric Infrastructure. See also Cisco's APIC Basic Configuration Guide for the policy-model configuration concepts.

QUESTION NO: 4

Which two options describe information that is included in the VXLAN VNID to identify forwarding information between the ingress nodes? (Choose two.)

A. APIC that set the VXLAN VNID.

B. Egress node that set the VXLAN VNID.

C. VRF context to which the packet belongs.

D. EPG from which the frame is sourced and the bridge domain to which this packet is forwarded.

E. List of spine and leaf nodes through which the packet flow.

ANSWER: C D

Explanation:

In Cisco ACI, the VXLAN network identifier is used as an overlay forwarding context. For routed traffic, the identifier represents the VRF context to which the packet belongs. This lets the receiving leaf switch perform the lookup in the correct tenant routing context and preserves tenant routing isolation as traffic crosses the IP fabric.

For bridged traffic, ACI uses the overlay context associated with the bridge domain to transport the frame to the appropriate destination location. The ingress leaf also classifies the source endpoint into its EPG, so the source EPG identity is available for ACI policy enforcement while the bridge-domain forwarding context identifies the Layer 2 forwarding domain. Together, source EPG classification and bridge-domain forwarding context allow the fabric to apply the intended contract and forwarding behavior from ingress through egress. Cisco describes ACI as using VXLAN-based encapsulation and distributed policy enforcement across the fabric. See the Cisco ACI architecture white paper and the Cisco APIC Layer 3 Networking Configuration Guide.

QUESTION NO: 5

What is the maximum number of configurable vPC links in an ACI fabric?

A. 16

B. 8

C. 4

D. 2

ANSWER: A

Explanation:

The maximum number of configurable vPC links is **16**. In Cisco ACI, a virtual Port Channel is formed by a pair of leaf switches that operate together to provide an active-active, loop-free attachment for a downstream device. The vPC construct allows the connected device to use port-channel member links spanning both leaves, while ACI maintains forwarding consistency and resiliency across the leaf pair. The ACI platform limit for this configuration is 16 vPC links for the applicable leaf-pair vPC configuration. This scale value is important when designing connectivity for dual-homed servers, firewalls, routers, or other Layer 2-attached devices: each vPC-connected endpoint or external device must be accounted for within the supported vPC-link capacity. Cisco documents vPC as an access-policy and interface-policy configuration used to provide redundant connections from endpoints to two leaf switches. For platform-specific scale considerations, engineers should also validate the software release and leaf-switch hardware in use, because supported scale is documented in Cisco's release and hardware guidance. See Cisco's ACI Layer 2 Configuration Guide: Configuring vPC and the Cisco APIC support documentation.

QUESTION NO: 6

How are VLAN tags used in an ACI fabric?

A. To group traffic in Layer 3 IP subnet.

B. To group traffic, in Layer 2 broadcast domains.

C. Only for traffic classification.

D. Only for reporting purposes.

ANSWER: B

Explanation:

In Cisco ACI, VLAN encapsulation is used at the fabric edge to associate incoming or outgoing Layer 2 traffic with an endpoint group and its associated bridge domain. A bridge domain defines the Layer 2 forwarding and broadcast domain in ACI, including such functions as MAC learning, flooding behavior, and the bridge-domain subnet configuration. When an endpoint group is statically bound to a leaf-interface path, the binding includes a VLAN encapsulation value. This value enables the leaf switch to classify frames received on that interface into the appropriate endpoint group; the endpoint group is then associated with its bridge domain and policy controls. Thus, VLAN tags provide the external/access-facing Layer 2 segmentation that maps connected workloads into the ACI logical networking model. The fabric itself uses VXLAN-based forwarding for traffic across leaf and spine switches, while VLAN encapsulation remains important for attachment and segmentation at access interfaces. Cisco documents VLAN pools as the source of VLAN encapsulation values used for endpoint-group static path bindings, and describes bridge domains as the Layer 2 constructs that contain endpoint-group forwarding behavior. See the Cisco APIC Basic Configuration Guide and the Cisco ACI VLAN Pools documentation.

QUESTION NO: 7

Which two events occur on the ACI fabric in the event of a downlink failure on one vPC peers when all local member ports are down? (Choose two)

A. The vPC reconfigures using the secondary peer link that is associated with the endpoints and a new VTEP entry is created.

B. A bounce entry is created for the endpoints that are reachable via the port channel that points to the VTEP of the peers.

C. The ACI fabric rediscovers the vPC peers and re-establishes communication between the endpoint and the leaf switch.

D. All MAC-to-leaf bindings for the specific vPC are removed from the COOP database and the spine proxy.

E. The APIC removes the associated leaf switch from inventory and rediscovers the fabric.

ANSWER: B D

Explanation:

When every local member link of a vPC port channel fails on one of the vPC leaf peers, that leaf can no longer provide local reachability for the endpoints learned through that vPC. ACI must promptly withdraw the affected endpoint location information so that traffic is not directed toward the failed local attachment. Therefore, all MAC-to-leaf bindings associated with that specific vPC are removed from the COOP database and from the spine proxy's endpoint mappings. This withdrawal lets the fabric use the remaining valid reachability information through the surviving vPC peer.

ACI also creates a bounce entry for endpoints reached through the port channel toward the peers' VTEP. The bounce mechanism is an endpoint-mobility and convergence safeguard: it causes endpoint traffic to be redirected or relearned appropriately rather than continuing to use stale forwarding information after the local vPC member links are lost. Together, the COOP/spine-proxy withdrawal and bounce entry provide rapid, loop-free endpoint convergence while preserving forwarding through the operational vPC peer. Cisco documents vPC behavior and endpoint forwarding concepts in the Cisco APIC Layer 2 Configuration Guide and the Cisco ACI endpoint learning white paper.

QUESTION NO: 8

Which in an ACI fabric can configure vPCs?

A. Tenant administrator

B. Server administrator

C. Network administrator

D. Infrastructure administrator

ANSWER: D

Explanation:

Infrastructure administrator is correct because Cisco ACI vPC configuration is an infrastructure-access function performed through APIC fabric access policies. The administrator creates a vPC protection group that identifies the two participating leaf switches, then associates the relevant switch profiles, interface profiles, and interface policy groups. The interface policy group is configured as a vPC-type bundle policy group and supplies the channel-group settings used by the leaf pair. These objects are part of the Fabric Access Policies area of APIC rather than tenant policy configuration. This separation is intentional: tenants define application connectivity constructs such as VRFs, bridge domains, application profiles, endpoint groups, and contracts, whereas the infrastructure administrator defines the physical fabric attachment and access-policy constructs that connect endpoints to the fabric. The vPC domain/protection group also ensures that the selected leaf nodes form the required vPC pair and that the associated interfaces are deployed consistently. Cisco's APIC Layer 2 Configuration Guide describes configuring vPCs through vPC protection groups and access-policy objects: Cisco APIC Layer 2 Configuration Guide—Configuring vPC. Cisco also documents Fabric Access Policies as the location for defining interface and switch policy constructs: Cisco APIC Access Policies Configuration Guide.

QUESTION NO: 9

What does an APIC health score of 100 indicate for a monitored object?

A. The object has no health degradation.

B. The object has a critical fault.

C. The object has reached its maximum supported scale.

D. The object is in an unacknowledged state.

ANSWER: A

Explanation:

The object has no health degradation. is correct. APIC calculates health scores for managed objects based on the faults and fault severities associated with those objects. A score of 100 represents a fully healthy state with no health-impacting faults.

As faults are raised, acknowledged, or cleared, APIC recalculates the health score for the relevant object and its parent objects. Health scores help administrators quickly identify degraded tenants, applications, fabric nodes, interfaces, and other managed resources. See the Cisco APIC Operations Guide.