

flooding has been turned on.

- 7.** B. In ACI, traffic is flooded based on an FTag tree to ensure a loop-free topology. Each ACI fabric contains multiple FTag trees.
- 8.** D. The Deployment Immediacy parameter setting On Demand delays enforcement of policy in hardware until ACI receives its first packet on the associated port. This can cause a minor delay in forwarding.
- 9.** C. Apply Both Directions and Reverse Filter Ports are both needed. Apply Both Directions signals to ACI that it needs to create a reverse rule. Reverse Filter Ports tells ACI to swap the source and destination ports when creating the reverse rule.
- 10.** B. Log is a directive.

Chapter 9

- 1.** A. When connecting ACI to a router (as opposed to a Layer 3 switch), there is very little to no benefit gained when using SVIs. There is also no use case for floating SVIs in this situation because there is minimal potential for workload movement when connecting to physical routers. Use of routed interfaces rules out deployment of further L3Outs from other VRFs on the same interface(s). Routed subinterfaces, on the other hand, enable reuse of physical interfaces for Layer 3 extension of regular user VRFs. Each encapsulation can be tied to a different L3Out.
- 2.** D. A route profile for interleak does not create Deny prefix-list entries and therefore does not prevent entry of routes that have already been learned on an L3Out and added to a leaf RIB from being distributed into BGP. Therefore, A is not an acceptable answer. Answers B

and C would prevent the border leaf switches from learning the 10.0.0.0/8 subnet in the first place and are therefore incorrect. Answer D is correct because BGP route reflection is the basis for external route distribution in ACI fabrics.

3. C. In this case, a vPC can be configured for connectivity to the firewall, and an L3Out can be deployed using SVIs to enable peering with the firewall. Floating SVIs is not the best choice because the question specifies that the firewall is a physical appliance, and therefore there is no expectation for firewall connections to move between switches.
4. C. The only parameters administrators need to enter for BGP route reflection in ACI are the BGP ASN the fabric should use and the spines in each pod that should function as route reflectors. All other configuration occurs in the background, without user input.
5. B, D. In this case, the administrator is experiencing a common problem. If the requirement is to implement multiple L3Outs in a single VRF, the administrator is advised to either use BGP to benefit from a separate route map per L3Out or to implement the EIGRP and OSPF L3Outs on different switches. This problem may at some point be resolved through an enhancement.
6. A. To use an ASN other than the route reflector ASN, an administrator needs to use a *local-as* configuration in the BGP peer connectivity profile to make its BGP AS look like something else to the peer.
7. A, D. EIGRP cannot be used on BGP L3Outs. For BGP loopback reachability, use OSPF or static routes on BGP L3Outs. B is incorrect because the BGP dynamic neighbor feature in ACI does not attempt to start a BGP

session but waits for the other side to try to initiate a session. Without explicit configuration on the other side, a session will never be established. Therefore, C is incorrect. A and D are the correct answers.

- 8.** B, C. Administrative distances for SPF are configured via an OSPF timer policy and are applied at the VRF level for all address families or at the VRF level for an individual address family. Therefore, A is incorrect. ACI does support OSPF authentication, which needs to be configured under an OSPF interface profile, so B is correct. Any border leaf L3Out leverages VRF-lite to extend routing to the outside world. Answer C is correct. ACI does support OSPFv3, but the system makes it mostly transparent from the user perspective. Just assign an IPv6 address to an L3Out, and the routing process reflects OSPFv3. For this reason, D is incorrect.
- 9.** A, D. BFD is not supported on BGP prefix peers and loopback addresses as of the time of writing. It is supported on non-loopback interfaces and all configurable routing protocols in ACI.
- 10.** A. The route profile type Match Routing Policy Only has more similarities with the **route-map** command in other solutions, but the default route profile type Match Prefix and Routing Policy does merge implicit and explicit route maps together.

Chapter 10

- 1.** B. In endpoint migration scenarios, it is best to set L2 Unknown Unicast setting to Flood to ensure similar forwarding behavior across ACI and the traditional network.

- 2.** D. Because an any-to-any contract typically creates a full mesh of relationships, this can impact the policy CAM.
- 3.** C. vzAny allows a one-to-many contract relationship within the scope of a VRF instance.
- 4.** A. Multi Destination Flooding is primarily concerned with forwarding of broadcast, L2 multicast, and link-local traffic.
- 5.** B. When implementing a bridge domain extension, only a single external Layer 2 EPG is allowed per bridge domain.
- 6.** A, C, D. There is no such thing as AAEP extension. AAEP EPG is a variant of EPG extension. The other three answers are all correct.
- 7.** B, C, D. Once the default gateway moves into ACI, the Layer 2 connection is irrelevant. Therefore, A is incorrect. However, if the L3Out has not been associated with the BD (or EPG) or the subnet Scope parameter has not been set to Advertised Externally, the subnet is not advertised out of ACI. For this reason, B and C are correct. Another possible reason for the communication outage may be contracts. With EPG extension, it is not ACI but the traditional network switches that initially control access to the subnet. But when the default gateway moves into ACI, contracts govern communication with the EPGs. For this reason, D is also a correct answer.
- 8.** A. Port Local Scope can be used to enable multiple EPGs to use the same encapsulation across different ports on a given leaf switch.
- 9.** D. All endpoints in a common flooding domain simultaneously experiencing performance degradation

could signal the possibility of a Layer 2 loop. Answer A is incorrect because if MCP had taken action, any offending ports would have been disabled. Answers B and C are incorrect because no administrative action is required to enable ACI to flood Rapid PVST+ BPDUs out all ports associated with the same EPG and encapsulation. Answer D is correct because the point-to-point Spanning Tree Protocol link type can lead to faster Spanning Tree Protocol convergence than what may be safe given the hub-like nature of ACI from a Spanning Tree Protocol perspective.

- 10.** A. ACI does need special configuration to ensure that MST BPDUs arriving in the native VLAN on interswitch links are not dropped, so answer A is correct. Answers B and C are incorrect because ACI does not run Spanning Tree Protocol, participate in the Spanning Tree Protocol topology, or even halt the flooding of BPDUs due to bridge domain setting modification. Answer D is a recipe for utter disaster. BPDU filtering, when used to prevent BPDU entry into ACI from outside switches, should only be implemented on external switches on interfaces that face ACI. This is because BPDU filtering prevents outbound advertisement of BPDUs. It should be used only when there will never be a second entry point for a VLAN into an ACI fabric.

Chapter 11

- 1.** D. Creating a port group for vCenter and its dependencies using the port binding setting Ephemeral allows the administrator to reassign the vCenter VM to the specified port group in the event that certain failure scenarios occur.

- 2.** B. The vSphere distributed switch is more advanced than the vSphere standard switch. Nexus 1000v and the AVS are not owned and managed by VMware.
- 3.** A. VMkernel adapters are logical interfaces that enable transmission, receipt, or processing of hypervisor system traffic. Examples of ESXi system traffic include management, vMotion, IP storage, fault tolerance, and vSAN.
- 4.** A, D. The only correct answers are A and D.
- 5.** C. The answer is data center.
- 6.** B. The VMM domain profile can be understood to be analogous with the VDS. A VDS needs to be generated before it can be consumed by ESXi hosts.
- 7.** A, B, D. The only incorrect answer is C because ACI does not push bridge domains into a VDS; it pushes EPGs into a VDS.
- 8.** C. The resolution immediacy setting Pre-Provision ensures that the policy is downloaded to the leaf switches with operational access policies involving the AAEP associated with the VMM domain, regardless of the status of hypervisors or LLDP and CDP neighbor relationships. The deployment immediacy setting Immediate would be needed to complement this.
- 9.** A. VDS names need to be unique across each vCenter instance.
- 10.** A. By creating an enhanced LAG policy and updating EPG VMM domain associations, an ACI administrator can create uplink port channels on an ACI-generated VDS and control the path that traffic takes.

Chapter 12

- 1.** D. Device packages designed for service policy mode typically enable a wide range of changes, sometimes to the extent that the entire appliance may be configured by ACI.
- 2.** B. Device packages are the foundation of both service policy mode and service manager mode.
- 3.** B. This statement accurately describes service graphs with PBR. Non-PBR service graphs, on the other hand, expect that users insert the services device into the topology using VLAN or VRF stitching.
- 4.** A. This process of operationalizing an instance of a service graph is called rendering.
- 5.** C. Go-through mode relates to deployment of transparent mode firewalls. Bridging between a single subnet with this deployment mode requires at least two bridge domains.
- 6.** D. A device selection policy determines which L4-L7 services device can be used for a given contract and service graph template.
- 7.** D. Setting the Locked attribute to True for a given parameter prevents users who need to consume a function profile from modifying the parameter via ACI.
- 8.** B. A service graph template is meant to be generic and does not specify EPGs. Instead, the instantiations of service graphs and the L4-L7 service graph to contract subject assignments determine the exact EPGs to which a function or service chain applies.
- 9.** A. When you select Virtual, ACI exposes a drop-down that necessitates selection of a VMM domain.
- 10.** D. Cluster interfaces, also called logical interfaces, are user-friendly mappings to a set of concrete interfaces.

The use of cluster interfaces allows other ACI configurations to reference something that is more memorable to users. It reduces the possibility of configuration mistakes because it limits the need to reference concrete interfaces after initially mapping them to cluster interfaces. Note that provider and consumer connectors themselves map back to cluster interfaces.

Chapter 13

- 1.** A. Out-of-band interfaces have been designed to be very difficult to impact through everyday configuration changes.
- 2.** B. In-band configurations are reliant on access policies. Hence, they are a lot more closely tied to configurations in the access policies view. Something like removing the in-band management encapsulation from the pertinent VLAN pool can theoretically trigger an outage within the in-band network.
- 3.** B. ACI does not allow leaking of data plane traffic into the oob VRF instance. However, it does allow leaking of traffic to and from the inb VRF.
- 4.** A. Cisco recommends that dynamic and static IP addressing not be combined when OOB and in-band management are deployed together.
- 5.** B. OOB management is designed to be simple. In-band management, on the other hand, allows more advanced constructs and features such as the deployment of L3Outs.
- 6.** C. NTP is not a prerequisite for in-band management.

- 7.** A. Managed node connectivity groups are constructs that map IP address pools to management EPGs. Therefore, the configuration of at least one managed node connectivity group is mandatory when using dynamic IP addressing.
- 8.** B. APICs function much like any other servers. They are not VRF aware and use route metrics to prefer one route over another.
- 9.** B. In-band contracts are standard contracts and are very much like contracts applied elsewhere within user VRFs. Out-of-band contracts offer less functionality. For example, they do not support the Log directive. They can also only be applied to OOB EPGs in the provided direction. Therefore, they do have minor differences.
- 10.** A. The APIC Connectivity Preferences setting changes the preferred management interface for outbound connections by manipulating route metrics.

Chapter 14

- 1.** B. System messages can also be generated for events and logs—specifically audit logs and session logs.
- 2.** C. System message formats include ACI and NX-OS. Of the two, the ACI system message structure is the more granular.
- 3.** C. Monitoring policies under the Access Policies view (the monInfraPol class) govern issues related to downlink (non-fabric) port failures. Access Policies also governs VMM management.
- 4.** A, D. For syslog communication to be possible, the syslog server needs to be configured as an external syslog collector or in a syslog monitoring destination

group. Furthermore, syslog source groups that reference the monitoring destination group need to be configured. Syslog is documented in RFC standards and is not associated with versions. Contracts for syslog are not always needed, especially when out-of-band is used as the management EPG. Regardless, answer C is incorrect because a permit-all contract would still enable syslog communication.

5. B. Custom monitoring policies do not take effect until they are manually allocated to a parent object. Through inheritance, all child objects that themselves do not have custom monitoring policy allocations then get assigned to the new custom monitoring policies.
6. C. **logit** is used to test syslog configurations within a fabric through submission of a test system message.
7. D. Regardless of the configuration status or whether there is full communication between ACI and the SNMP manager, ACI does not support SNMP write commands. Therefore, an SNMP manager would never be able to use SNMP to make configuration changes to ACI.
8. B, C. Answer A is not a possible reason for communication to fail. Contracts just need to be broad enough to allow the desired communication. Answer B is a reason for SNMP communication failing. ACI supports a maximum of 10 trap receivers. If more are configured, two of the receivers will not function. The SNMP policy enforces ACL-like security, and the *only* client entries that must be populated in the Client Entries field are the IP addresses of the SNMP managers.
9. C. Certain MIBs that touch on VRF-specific parameters require that the VRF instance be associated with an SNMP context for SNMP read queries to function.

- 10.** C. By default, SNMP get or read queries take place over UDP port 161, and SNMP traps flow over UDP port 162.

Chapter 15

- 1.** C. The tenant-admin role maps to a wide range of privileges, which means it is a very powerful default role within ACI. With this role and the access privilege type set to Write, there is very little a user cannot do within the specified tenants. For example, the user can create L4-L7 devices within the Prod1 and Prod2 tenants as long as the user has also been associated with relevant domains, and the user can apply service graphs. The user can also create basic objects within these tenants. However, the user cannot map encapsulations to switch ports unless he has also been granted access to the underlying hardware. Note that all tenant users gain read-only access to the common tenant by default.
- 2.** A. The ops role provides network operator privileges to an ACI fabric, enabling basic monitoring and troubleshooting functionalities.
- 3.** B. Several security domains are predefined: all, mgmt, and common. The predefined security domain all provides access to the entire ACI object hierarchy.
- 4.** B. RBAC rules cannot be used to deny users access. If a user has too much access, the roles, privileges, security domains, and privilege types allocated to the user should be revisited.
- 5.** A. A privilege enables access to a particular function within the system. An ACI fabric enforces access

privileges at the managed object (MO) level. A role is simply a collection of privileges.

- 6.** D. Just as with almost everything else in ACI, the goal with RBAC rules is to templatize configurations. ACI therefore attempts to enable users to expand security domain access to users associated with the security domain by allowing access to additional DNs. Therefore, parameters required for creating an RBAC rule consist of the DN of the additional object, the security domain to be expanded, and whether to grant users write or simply read-only access to the new portion of the object hierarchy.
- 7.** C. The access-admin role enables administration and configuration of access policies.
- 8.** A, C, D. The answers are self-explanatory.
- 9.** C. The first option provides the user administrative access to the entire ACI object hierarchy but with read-only privileges, which is mostly useful for network operator CLI access. The second option provides the user the aaa role with write privileges and the tenant-admin role fabricwide but with read-only privileges. The third option provides full administrative access to the fabric. The fourth option is incorrectly formatted.
- 10.** B. Users can still leverage the fallback login domain. If the fallback login domain has not been modified from its default setting, users can authenticate against the local database within ACI by using a special login syntax.

Chapter 16

- 1.** C. MP-BGP EVPN handles cross-site endpoint information advertisements.

- 2.** B. ACI Multi-Site uses OSPF to build the underlay.
- 3.** B. ACI Multi-Site only governs tenants. Access policies continue to be configured locally within APICs. Not all tenant objects can currently be deployed from MSO, but when a tenant has been imported into MSO, administrators should refrain from making changes to objects within the MSO-managed tenant.
- 4.** B. ACI Multi-Site defines a unit and scope of a change using templates.
- 5.** A. If the fabrics have already been integrated into ACI Multi-Site, the only thing you need to do is to create a schema with templates underneath it and then add the necessary contracts to the EPGs to enable communication. Proper routing within VRF instances should also be set up.
- 6.** D. Host-based routing can allow for optimization of ingress traffic, ensuring that traffic ingresses the data center where the endpoint resides.
- 7.** A. ACI Multi-Site enables IP mobility across sites without the need to carry over performance-limiting and dangerous forwarding methods such as flooding.
- 8.** A. ACI Multi-Pod is a good fit for a lot of active/active use cases such as DRS. These requirements are not supported with ACI Multi-Site.
- 9.** A. ACI Multi-Pod is a good fit for a lot of active/active use cases such as active/active firewall clustering. This requirement is not currently supported with ACI Multi-Site.
- 10.** B. ACI Multi-Site integrates with the Cisco Cloud APIC and manages the public cloud deployment as yet another site under its management.

Appendix B

CCNP Data Center Application Centric Infrastructure DCACI 300- 620 Exam Updates

Over time, reader feedback allows Pearson to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new materials clarifying and expanding on those troublesome exam topics. As mentioned in the Introduction, the additional content about the exam is contained in a PDF on this book's companion website, at <http://www.ciscopress.com/title/9780136602668>.

This appendix is intended to provide you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content. This appendix attempts to fill the void that occurs with any print book. In particular, this appendix does the following:

- Mentions technical items that might not have been mentioned elsewhere in the book

- Covers new topics if Cisco adds new content to the exam over time
- Provides a way to get up-to-the-minute current information about content for the exam

Always Get the Latest at the Book's Product Page

You are reading the version of this appendix that was available when your book was printed. However, given that the main purpose of this appendix is to be a living, changing document, it is important that you look for the latest version online at the book's companion website. To do so, follow these steps:

Step 1. Browse to

www.ciscopress.com/title/9780136602668.

Step 2. Click the **Updates** tab.

Step 3. If there is a new [Appendix B](#) document on the page, download the latest [Appendix B](#) document.

Note

The downloaded document has a version number. Comparing the version of the print [Appendix B](#) (Version 1.0) with the latest online version of this appendix, you should do the following:

- **Same version:** Ignore the PDF that you downloaded from the companion website.
- **Website has a later version:** Ignore this [Appendix B](#) in your book and read only the latest version that you

downloaded from the companion website.

Technical Content

The current Version 1.0 of this appendix does not contain additional technical coverage.

Glossary

A

access policy A policy that primarily governs the configuration and operation of non-fabric (access) ports. Configuration of parameters such as link speed, CDP, LLDP, and LACP for connectivity to downstream servers, appliances, or non-ACI switches, as well as routers all fall into the realm of access policies. Access policies also include mechanisms to allow or block the flow of tenant traffic on access ports.

ACI Multi-Pod The natural evolution of the ACI stretched fabric design in which spine and leaf switches are divided into pods, and different instances of IS-IS, COOP, and MP-BGP protocols run inside each pod to enable a level of control plane fault isolation.

ACI Multi-Site A solution that interconnects multiple ACI fabrics for the purpose of homogenous policy deployment across ACI fabrics, homogenous security policy deployment across on-premises ACI fabrics and public clouds, and cross-site stretched subnet capabilities, among others.

Any EPG (vzAny) A one-to-all EPG relationship that provides a convenient way of associating all endpoint groups (EPGs) in a VRF instance with one or more contracts.

APIC Cisco IMC A controller that allows lights-out management of the physical server, firmware upgrades, and monitoring of server hardware health.

APIC cluster A set of three or more servers that connects to leaf switches within an ACI fabric and functions as the central management point for the entire fabric.

APIC in-band port APIC VIC adapters that need to be directly cabled to ACI leaf switches to allow fabric initialization and switch discovery. The VIC adapters used for in-band communication operate at 10 or 25 Gigabit Ethernet speeds.

APIC OOB port An embedded LAN on motherboard (LOM) port for out-of-band management of an APIC. In third-generation APICs, these dual LAN ports support both 1 and 10 Gigabit Ethernet. The OOB ports are the default avenue for management access to an ACI fabric.

application profile A container that allows EPGs to be grouped according to their relationship with one another to simplify configuration and auditing of relevant policies and to enable a level of policy reuse.

ARP gleaning A process in which ACI attempts to “tickle” potential silent hosts by sending ARP traffic toward them, enabling ACI to then learn of such hosts in the data plane. Also known as silent host detection.

attachable access entity profile (AAEP) A construct that fabric administrators use to authorize the placement of endpoint traffic on external entities, such as bare-metal servers, virtual machine hypervisors, switches, and routers. ACI can connect to external entities using individual ports, port channels, or vPCs.

audit log A record of user actions in ACI, such as logins, logouts, object creations, object deletions, and any other configuration changes (object attribute changes).

B

BGP EVPN router ID An ID for each spine that has been enabled for ACI Multi-Site forwarding that enables route peering across sites.

blacklisting The practice of forwarding all traffic except traffic that is blocked using tools like access lists. The default behavior of traditional switches and routers is to blacklist traffic.

border leaf A leaf switch that provides Layer 2 and Layer 3 connectivity to outside networks. Border leaf switches are often the point of policy enforcement between internal and external endpoints.

bridge domain (BD) A Layer 2 forwarding construct that is somewhat analogous to a VLAN and has to be associated with a VRF instance.

C

class One or more objects in the MIM that are of a similar type.

CloudSec encryption Encryption used when traffic is egressing a fabric through multisite spines and is destined for spines in another fabric and needs to be encrypted. This is a VTEP-to-VTEP encryption feature.

compute leaf An ACI leaf switch that connects to a server. Compute leaf switches are the point of policy enforcement when traffic is being sent between local endpoints.

concrete device An L4–L7 services appliance that is used in a service graph.

consumer In a client/server communication, the device initiating a communication request.

contract A mechanism that references one or more subjects and is associated directionally with EPGs to determine which traffic flows are bound by the contract. Contracts are scope limited and can also be configured to modify traffic QoS markings.

contract scope A condition that determines whether a contract can be enforced between EPGs. Contract scope options include application profile, VRF, tenant, and global.

D

deployment immediacy When policies, such as VLANs, VXLAN bindings, contracts, and filters, have been downloaded to a leaf switch, factors that specify when a policy is actually pushed into the hardware policy content-addressable memory (CAM).

device manager A configuration that tells ACI how to access an L4–L7 services device management solution for services appliance configuration in service manager mode. A device manager configuration includes the IP address, communication protocol, and credentials for the L4–L7 management solution.

device selection policy A policy that associates or ties one or more L4–L7 devices to a graph template and contract. Also known as a logical device context.

distinguished name (DN) A unique name that describes an ACI-managed object and locates its place in the ACI object hierarchy.

domain The central link between the access policies hierarchy and the tenant hierarchy. A domain is the glue that binds tenant EPGs to access and virtual networking policies. With the help of pools, domains determine whether a tenant administrator is allowed to map an EPG to a certain encapsulation and underlying infrastructure. Each domain points to and consumes a single VLAN pool.

dynamic breakout port A high-bandwidth port on certain hardware platforms that is split into multiple lower-speed connections, allowing customers to use a greater amount of the forwarding capacity of a high-bandwidth port even when there is a need to attach lower-bandwidth endpoints.

dynamic tunnel endpoint (DTEP) Dynamically learned TEP addresses that include PTEPs and spine proxy addresses.

dynamic VLAN allocation ACI's automatic choice of a VLAN ID out of a range of VLANs associated with a VLAN pool mapped to an EPG.

E

endpoint Especially in the context of local endpoint learning, one MAC address and zero or more IP addresses associated with the MAC address. In remote endpoint learning, a cached IP address or MAC address of a device.

endpoint group (EPG) A group of physical or virtual network endpoints that reside within a single bridge domain and have similar policy requirements. Endpoints within an EPG may be directly or indirectly attached to ACI leaf switches but communicate in some fashion over an ACI fabric.

event record An object that is created by a system to log the occurrence of a specific condition that might be of interest to ACI administrators.

external bridge domain A type of domain used in attachments to switches outside ACI for Layer 2 connectivity.

external bridged network A bridge domain extension out an ACI fabric. Also referred to as an L2Out.

external EPG A special type of EPG that represents endpoints outside an ACI fabric, such as user laptops, campus IoT devices, or Internet users. External EPGs allow the application of different security policies to different sets of outside users. External EPGs classify outside traffic using subnets, but the subnets can be as granular and numerous as needed.

external routed domain A type of domain used in attachments to switches and routers outside ACI for Layer 2 connectivity.

F

fabric policy A policy that governs configurations that apply more holistically at the switch or pod level. Fabric policies also include the operation and configuration of switch fabric ports.

fabric port An interface that is used to interconnect spine and leaf switches within a fabric. By default, all spine switch interfaces besides the mgmt0 port and a number of leaf uplink ports are configured as fabric ports.

fabric tunnel endpoint (FTEP) A single fabricwide pervasive IP address. ACI creates loopback 1023 interfaces on all leaf switches for assignment of FTEP addresses. The FTEP address represents the entire fabric and is used to encapsulate traffic in VXLAN to and from AVS and AVE virtual switches, if present.

fault A potential problem in a fabric or the lack of required connectivity outside the fabric. Each fault has a weight and a severity and is registered into the ACI object hierarchy as a child object to the MO primarily associated with the fault.

fault lifecycle policy A policy that specifies the timer intervals that govern fault transitions between states in the lifecycle. Fault lifecycle policies can be specified in the Common policy, in default policies, or in a custom monitoring policy.

filter A mechanism that matches interesting traffic flows. The EtherType, Layer 3 protocol type, and Layer 4 ports involved in communication flows can all be used to match interesting traffic using filter entries.

floating SVI A feature that enables users to configure an L3Out without locking the L3Out down to specific physical interfaces. This feature enables ACI to establish routing adjacencies with virtual machines without having to build multiple L3Outs to accommodate potential VM movements.

forwarding tag (FTag) tree A predefined topology based on which ACI is able to forward multi-destination traffic. Each FTag tree does not necessarily use all fabric uplinks. That is why ACI creates multiple FTag trees and load balances multi-destination traffic across them.

function profile The main mechanism by which L4-L7 services device administrators define configuration

parameters in ACI to feed back to services devices.

G

global scope MIB An MIB whose scope is not limited to a specific VRF instance and that touches on broader aspects of the fabric. Examples of MIBs of a global scope are those that request data related to the status of switch power supplies, interface or port channel statuses, CPU utilization, and memory utilization.

H

health scores Scores that enable an organization to evaluate and report on the health and operation of managed objects, switches, tenants, pods, or the entire ACI fabric. By associating a weight with each fault, ACI provides a means for allocating health scores to objects. An object whose children and associated objects are not impacted by faults has a health score of 100. As faults occur, the health score of the object diminishes until it trends toward 0. With the resolution of all related faults, the health score returns to 100.

I-J-K

infrastructure VLAN A VLAN that is used for control communication between ACI fabric nodes (leaf switches, spine switches, and APICs). This VLAN is also used for extending an ACI fabric to AVS or AVE virtual switches. The infra VLAN should be unique and should not be used elsewhere in the environment. Acceptable infra VLAN IDs are 2 through 4094.

interface policy In ACI, configuration parameters that dictate interface behavior. Examples of interface policies include port speeds, enabled or disabled protocols or port-level features, and monitoring settings.

interface policy group A port configuration template that aligns with link types. Each individual physical interface or link aggregation within ACI derives two critical configuration components from an interface policy group: a collection of interface policies and an AAEP. Some types of interface policy groups are fully reusable, and others are semi-reusable.

interface profile A collection of interface mappings that gets bound to switch IDs through its association with one or more switch profiles.

interface selector A child object of an interface profile that ties an interface policy group to one or more port IDs. Since switch associations are determined by switch profiles and not interface profiles, interface selectors only determine port ID associations and not the list of switches to which the interface policy groups should be assigned.

interleak Redistribution of all L3Out-learned routes within user VRF instances into BGP for advertisement across the fabric. If an L3Out is using BGP, no redistribution (interleak) is required.

intersite L3Out In current MSO releases, a feature that enables endpoints located in one site to use a remote L3Out to connect to entities in an external network.

intra-fabric messaging (IFM) An encrypted in-band communication channel between APICs and switches over the infrastructure VLAN. When APICs push policy to switches, all relevant communication rides the IFM channel.

IP storage leaf An ACI leaf switch that connects to an IP storage system. IP storage leaf switches can be a point of policy enforcement for traffic to and from local endpoints.

L

L2 Unknown Unicast A setting for unicast traffic destined to an endpoint whose MAC address cannot be found in the ACI endpoint table.

L3Out An object that defines a routed connection or a series of routed connections outside an ACI fabric to allow route propagation between a VRF instance within ACI and the outside world. BGP, OSPF, and EIGRP are all supported protocols for use on L3Outs. Static routes pointing outside ACI can also be configured on L3Outs.

L3Out bridge domain (BD) A domain that ACI creates internally for an SVI to provide a Layer 2 flooding domain. This BD is called an L3Out BD or external BD and is not visible to ACI administrators.

leaf A type of switch that is used as an attachment point for a server. APICs also connect to leaf switches.

leaf interface override A policy that allows interfaces that already have interface policy group assignments to apply an alternate interface policy group.

Link Debounce Interval A link-level policy setting that delays reporting of a link-down event to a switch supervisor.

local endpoint An endpoint that an ACI leaf learns from an access (non-fabric) port, even if the endpoint is not directly attached to the leaf.

logical device Physical devices clustered together. Also known as a clustered device.

logical interface profile A profile that consists of one or more logical interface profiles defining L3Out interfaces, interface IP addresses, MTU values for routing protocol peering, and any other interface-specific configuration parameters.

logical node profile An object that specifies which switches will establish routed connectivity to external devices for a given L3Out.

M

managed object (MO) An object or group of objects within a hierarchical tree. MOs are abstractions of fabric resources. An MO can represent a physical object, such as a switch, an interface, or a logical object, such as an application profile, an endpoint group, or a fault.

Management Information Base (MIB) An object that defines the information that a remote SNMP manager can request from an SNMP agent.

Management Information Model (MIM) An object hierarchy that is managed by and stored on the APICs that represents both physical and logical components of the ACI fabric.

MisCabling Protocol (MCP) An ACI protocol that detects loops caused by devices attached to an ACI fabric and that can be applied on both physical Ethernet interfaces and port channel interfaces.

monitoring destination group A syslog group that is used to define and group together syslog servers or SNMP servers.

monitoring source A definition added to a monitoring policy that points to the monitoring destination groups, thereby defining which server and server settings should be used for each set of monitoring policies.

monPolDn An object attribute that references a monitoring policy object.

MOQuery The CLI-based equivalent of Visore, which can be used to gain an understanding of the object hierarchy in ACI.

Multi Destination Flooding A setting that primarily addresses forwarding of broadcast, L2 multicast, and link-local traffic. The three configuration options for the Multi Destination Flooding parameter are Flood in BD, Drop, and Flood in Encapsulation.

multitenancy The ability to logically separate management as well as data plane forwarding of different logical environments that reside on top of common physical infrastructure.

N

network policy mode A service graph management model which requires that ACI configure network connectivity to an L4-L7 services device but not the L4-L7 device itself.

node ID A logical representation of an ACI switch or APIC that can be associated with or disassociated from physical hardware.

O

overlay multicast TEP A single anycast tunnel endpoint within each fabric (site) for ingress replication of cross-site data plane BUM traffic.

overlay unicast TEP A single anycast TEP address assigned to each pod within each fabric for forwarding of cross-site unicast traffic.

P-Q

pervasive gateway An anycast default gateway that ACI leaf switches install to allow local endpoints to communicate beyond their local subnets.

pervasive route A route to a BD subnet that points to the spine proxy TEP as its next-hop IP address. The function of a pervasive route is to ensure that a leaf switch knows that a particular destination is expected to be inside the fabric.

physical domain A domain that governs the attachment of bare-metal servers and appliances that need static VLAN allocations.

physical tunnel endpoint (PTEP) A type of IP address that ACI assigns to the loopback 0 interface of a given switch. Tunnels established between leaf switches for the purpose of data plane traffic forwarding are sourced from and destined to PTEP addresses.

platform-independent VLAN (PI VLAN) A VLAN ID that is locally significant to each leaf switch and represents a bridge domain or EPG for internal operations. PI VLANs are not used for traffic forwarding.

pod policy group A group of individual protocol settings that is collectively applied to a pod.

pod profile A construct that specifies date and time, podwide SNMP, Council of Oracle Protocol (COOP) settings, and IS-IS and Border Gateway Protocol (BGP) route reflector policies for one or more pods. Pod profiles map pod policy groups to pods by using pod selectors.

pod selector An object that references the pod IDs to which pod policies apply. Pod policy groups get bound to a pod through a pod selector.

Policy Universe The top level of the MIM hierarchical object tree. It is not the true root of the tree but is a key branch of the overall hierarchy representing the bulk of user-configurable policies.

port binding A setting that determines when virtual machines in a port group get allocated to a virtual port on a VDS.

port channel member override A policy used when an override needs to be applied to one or more links that are part of a port channel or vPC but not necessarily the entire port channel or vPC. Examples of port channel member overrides are implementation of LACP fast timers and modification of LACP port priorities.

port encapsulation VLAN A VLAN ID an administrator uses when mapping an EPG to a switch port. Both static path mapping and AAEP EPGs leverage this VLAN type. The term *port encapsulation* implies that the VLAN encapsulation used appears on the wire. Also known as an access encapsulation VLAN.

port group A group of ports with similar policy requirements.

preferred group member A feature that allows a set of EPGs within a VRF instance to have open communication with one another without the need for contracts while continuing to enforce contract requirements on all other EPGs within the VRF instance.

privilege An authorization that enables access to a particular function within a system. An ACI fabric enforces access privileges at the managed object (MO) level.

provider In a client/server communication, the device responding to a client communication request.

R

RBAC rule A rule that allows granular control on top of the existing RBAC framework within ACI. An RBAC rule allows the addition of desired subtrees of the ACI object hierarchy to a security domain to enable broader visibility to users who may be granted access to a given security domain.

remote endpoint An endpoint that a leaf learns by checking the source MAC and/or source IP header of a packet that arrives on a fabric port (over tunnel interfaces).

resolution immediacy Factors in ACI that define when policies such as VLANs, VXLAN bindings, contracts, and filters are downloaded to leaf switches.

role A collection of privileges in ACI. ACI has a set of predefined roles, but you can modify the predefined roles or expand on default ACI roles by creating custom roles.

route profile A profile that enables users to add user-defined match rules or set rules for route filtering or route manipulation. They are sometimes referred to as route control profiles or route maps.

route reflector A BGP speaker that is allowed to advertise iBGP-learned routes to certain iBGP peers. Route reflection bends the rules of BGP split horizon just a little, introducing a new set of BGP attributes for route loop prevention. In ACI, spines can be configured as route reflectors.

S

scheduler Software that allows administrators to specify a window of time for ACI to execute certain operations such as switch upgrades and configuration backups. Schedulers can be triggered on a one-time-only basis or can recur on a regular basis.

schema A collection of configuration templates and the assignment of each template to sites defined in the Multi-Site deployment.

secondary IP address An IP address that is used when an external device behind an L3Out needs to point a static route to a common IP address that a pair of border leaf switches respond to.

security domain A tag that references one or more subtrees in the ACI object hierarchy. After you create a security domain, you can assign it to tenants and domains. For more granular references, you can map a distinguished name (DN) in the ACI object hierarchy to a security domain. A user who is subsequently mapped to the security domain gains a level of access to the referenced subtrees of the object hierarchy.

service chain A succession of functions enforced through contracts.

service graph A graph of communication flows that are enforced via contracts to mandate the flow of traffic between a given pair of EPGs through a series of services functions.

service graph template A template that defines the desired functions through which certain traffic should flow without actually specifying the traffic (EPGs) to which it applies.

service leaf A leaf switch that connects to Layer 4–7 services appliances, such as firewalls and load balancers.

service manager mode A service graph management model that enables services administrators to make services configuration changes in the L4–L7 management tool provided by a device vendor. ACI automates configuration to the services device but only minimally configures the L4–L7 services device itself.

service policy mode A service graph management model that requires ACI to configure both network connectivity to an L4–L7 services device and also the L4–L7 device itself.

shadow EPG Any form of EPG that is automatically generated by ACI, typically for the purpose of automating enforcement of contracts between two components.

sharding Horizontal partitioning of databases that involves distributing a database across multiple instances of the schema. Sharding increases both redundancy and performance because a large partitioned table can be split across multiple database servers. It also enables a scale-out model involving adding to the number of servers as opposed

to having to constantly scale up servers through hardware upgrades.

site An independent ACI fabric.

site ID A unique numeric identifier for each fabric. Once selected, the site ID cannot be changed.

SNMP notification A notification that an SNMP agent sends to configured SNMP managers when an important system event occurs on an SNMP-enabled device.

SNMP trap An unreliable message that does not require an acknowledgment from the SNMP manager.

spine A type of switch that serves to interconnect leaf switches at high speeds and also handle certain control plane functions within a fabric.

squelching The process of suppressing faults or events of a specific fault code or event type, which helps reduce the noise from a monitoring perspective and allows a company to focus on the faults that really matter.

static VLAN allocation An administrator's static mapping of a specific EPG to a VLAN ID on a port, a port channel, a virtual port channel, or all ports on a switch.

stretched Objects, such as tenants, VRF instances, EPGs, bridge domains, subnets, or contracts, that are deployed to multiple sites.

stretched ACI fabric A partially meshed design that connects ACI leaf and spine switches distributed in multiple locations. The stretched ACI fabric design helps lower deployment costs when full-mesh cable runs between all

leaf and spine switches in a fabric tend to be cost-prohibitive.

subject A mechanism that determines the actions taken on interesting traffic or defines whether corresponding ports for return traffic should be opened.

system message A specially formatted message that typically contains a subset of information about a fault, an event, or another log record in the fabric.

switch profile A collection of switch policy group-to-node ID mappings that binds policy to switch IDs using switch selectors. Switch profiles reference interface profiles and deploy the port configurations defined in the interface profiles to switches to which the switch profile is bound. There are two types of switch profiles: leaf profiles and spine profiles.

switch selector A child object of a switch profile that associates a switch policy group to one or more node IDs.

T

template A child of a schema that contains configuration objects that are either shared between sites or are site specific. Each template gets associated with a single tenant. A template defines the unit or scope of a configuration change.

template conformity A feature of ACI Multi-Site that runs checks to validate that configurations under a template pushed to multiple sites by the MSO have not been altered within a given fabric by administrators.

tenant In ACI, a secure and exclusive virtual computing environment that forms a unit of isolation from a policy perspective but does not represent a private network.

TEP pool A subnet used for internal fabric communication. This subnet can potentially be advertised outside ACI over an IPN or ISN or when a fabric is extended to virtual environments using the AVS or AVE. TEP pool subnets should ideally be unique across an enterprise environment. Cisco recommends that TEP pool subnet sizes be between /16 and /21. TEP pool sizes impact pod scalability. Each pod should be assigned a separate TEP pool.

transit leaf A leaf switch that provides connectivity between two sites in a stretched fabric design. Transit leaf switches connect to spine switches in both sites. No special configuration is required for transit leaf switches. At least one transit leaf switch must be provisioned in each site for redundancy reasons.

U-V-W

user tenant A tenant that does not come out of the box with ACI and is created by a user.

Virtual Machine Manager (VMM) domain A type of domain that enables the deployment of EPGs and corresponding encapsulations into virtualized environments.

virtual routing and forwarding (VRF) instance A mechanism used to partition a routing table into multiple routing tables for the purpose of enabling Layer 3 segmentation over common hardware. In ACI, each tenant can contain multiple VRF instances.

Visore A GUI-based tool that can be used to gain an understanding of the object hierarchy in ACI.

VLAN pool The range of VLAN IDs that are acceptable for application to ACI access (non-fabric) ports for a particular function or use.

VM vNIC Virtual network adapters configured within VMs and associated with port groups.

VMkernel adapter A logical interface that enables transmission, receipt, or processing of hypervisor system traffic. Examples of ESXi system traffic include management, vMotion, IP storage, fault tolerance, and vSAN. Like virtual machines, VMkernel adapters need to be associated with port groups.

vmnic A physical network interface card that connects an ESXi server to a physical switch. You can think of a vmnic as a string used in the naming of virtual switch uplinks within ESXi hypervisors.

vPC peer dead interval The amount of time a leaf switch waits following a vPC peer switch failure before it assumes the role of vPC master. The default peer dead interval in ACI is 200 seconds. This value can be tuned to between 5 and 600 seconds through configuration of a vPC domain policy.

VRF-specific MIB An MIB whose scope is limited to a VRF instance. Examples of VRF-specific MIBs are those involving IP addresses or endpoints residing in a VRF or route peerings out of a specific VRF.

vSphere distributed switch (VDS) A virtual switch that is created and centrally managed by vCenter, with the switch data plane residing within the ESXi hypervisors.

vSphere load balancing Load balancing in vSphere that enables administrators to choose how uplink ports on a virtual switch are used to distribute network traffic originating from virtual machines and VMkernel interfaces.

vSphere standard switch (vSwitch) A basic Layer 2 virtual switch instantiated by and limited in scope to a single hypervisor. It can be used to enable ESXi host IP connectivity with other hosts or endpoints. It can also enable basic connectivity for virtual machines.

whitelisting The practice of dropping all traffic unless it is explicitly allowed via contracts. The default behavior of ACI and firewalls is to support whitelisting.

X-Z

zero trust security An approach to network security in which communication is allowed only if there is a justification for the traffic flows. ACI supports a zero-trust architecture through whitelisting and the ability to selectively punt traffic to firewalls for identity verifications, where necessary.

Index

Symbols

- | (pipe) delimiter character, [416](#)
- 802.1Q standard (IEEE)**, [7](#)
- 802.1X authentication**, [173](#), [175](#)

A

AAA (access, authentication, and accounting), [106](#).
See also [access methods](#); [access policies](#)

- EIGRP (Enhanced Interior Gateway Routing Protocol)
 - authentication, [324](#)
- external AAA server integration, [532](#)
 - AAA authentication policy settings*, [547–550](#)
 - ACI configuration for LDAP*, [541–547](#)
 - ACI configuration for RADIUS*, [540–541](#)
 - ACI configuration for TACACS+*, [532–536](#)
 - Cisco AV pair formatting*, [538–540](#)
 - ISE (Identity Service Engine) configuration*, [536–538](#)
- RBAC (role-based access control) access, [133](#)
 - user access
 - granting*, [523–525](#)
 - modifying*, [523–525–528](#)
- aaa role**, [520](#)

aaaSessionLR class, 128

AAEPs (attachable access entity profiles), 165-169, 382

configuration, 167-169, 190-191

definition of, 589

EPGs (endpoint groups), 207-210

in-band management configuration, 468

in L3Out domains, 302

overview of, 165-166

Access (802.1P) port-binding mode, 268

Access (Untagged) port-binding mode, 268

access, authentication, and accounting. *See AAA (access, authentication, and accounting)*

access encapsulation VLANs, 246

access methods

API (application programming interface), 103

CLIs (command-line interfaces)

APIC CLI, 100-102

overview of, 100

switch CLI, 102-103

GUI (graphical user interface), 99, 107-108

management access modification, 103-105

overview of, 98-99

access policies. *See also AAA (access, authentication, and accounting); domains; profiles*

AAEPs (attachable access entity profiles), 165-169, 382

configuration, 167-169, 190-191

definition of, 589

EPGs (endpoint groups), [207-210](#)
in-band management, [468](#)
in L3Out domains, [302](#)
overview of, [165-166](#)

ACI switch port configurations

- AAEP EPGs (endpoint groups)*, [207-210](#)
- implications of*, [210](#)
- individual port configuration*, [188-196](#)
- overview of*, [186-188](#)
- port channel configuration*, [196-201](#)
- vPC (virtual port channel) configuration*, [204-207](#)
- vPC (virtual port channel) domains*, [201-204](#)

for APIC in-band interfaces, [468-469](#)

BPDU Guard/BPDU Filter, [230-231](#)

configuration with quick start wizards, [211](#)

- Configure Interface, PC, and VPC Wizard*, [211](#)
- Configure Interface wizard*, [211-212](#)

CoPP (Control Plane Policing), [225-229](#)

definition of, [158](#), [589](#)

DHCP relay configuration, [219-221](#)

dynamic breakout port configuration, [215-217](#)

Error Disabled Recovery Policy, [231-232](#)

FEX (fabric extender) configuration, [212-215](#)

hierarchy of, [183-184](#)

interface policies and interface policy groups, [169-174](#)

- CDP (Cisco Discovery Protocol)*, [190](#)
- definition of*, [593](#)

deployment of, [173-174](#)

EIGRP (Enhanced Interior Gateway Routing Protocol), [321-323](#)

link level, [189](#)

LLDP (Link Layer Discovery Protocol), [189](#)

OSPF (Open Shortest Path First), [326-327](#)

overview of, [169-170](#)

port channel, [198](#)

types of, [170-173](#)

vPC (virtual port channel), [205-206](#)

leaf interface override policy, [232](#), [594](#)

MCP (MisCabling Protocol), [221-222](#), [594](#)

overview of, [158](#)

port channel member overrides, [232-235](#), [596](#)

QoS (quality of service) global class settings, [217-219](#)

selectors, [176-179](#)

stateless networking, [182-183](#)

storm control, [223-224](#)

switch policies and switch policy groups, [174-176](#)

tenancy and, [184](#)

VLAN pools, [159-160](#)

creating, [159-160](#)

designs for, [161-163](#)

overlap between, [164-165](#)

static versus dynamic VLAN allocation, [159](#), [598](#)

VLAN ranges in, [160](#)

access-admin role, [520](#)

access-list access-list-inbound extended permit icmp any any command, 460

Account Expires setting (User Identity), 523

Account Status setting (User Identity), 523

accounting. See AAA (access, authentication, and accounting)

ACI (Application Centric Infrastructure), benefits of, 9-16

architectural possibilities, 15

cross-platform integrations, 15

health monitoring and enhanced visibility, 16

multitenancy, 11-14

network management touchpoints, 9-10

policy reuse, 16

programmability, 11

scalability optimizations, 10

stateless networks, 11

traffic flow optimizations, 10

zero-trust security, 14-15

ACI Anywhere

ACI Multi-Pod

active/active data center deployments, 562-564

definition of, 589

overview of, 15, 25-26

stateful-services integration, 563-564

ACI Multi-Site, 555-558

cross-site connectivity, 555-557

extending ACI to remote locations and public clouds, [564](#)

locally governed configurations, [557](#)

MSO-governed configurations, [557](#)

primary and disaster recovery data center deployments, [558-562](#)

schemas, [557-558](#)

stateful-services integration, [563-564](#)

terminology for, [557](#)

extending ACI to remote locations and public clouds, [564-565](#)

with ACI Multi-Site, [564](#)

with remote leaf switches, [564-565](#)

with vPod, [564](#)

overview of, [552](#)

ACI fabric initialization

backups and restores

configuration backups, importing, [80-82](#)

configuration exports, [75](#)

configuration imports, [75-76](#)

configuration rollbacks, [82-83](#)

configuration snapshots, [80](#)

on-demand backups, [76-79](#)

scheduled backups, [79-80](#)

Cisco FabricPath, [7](#)

connectivity outside, [151-153](#)

external EPGs (endpoint groups), [151-153](#)

Layer 3 Outside (L3Out), [153](#)

endpoint movements within ACI fabric, [247](#)
fabric policies, [106](#), [592](#)
fabric ports, [23](#), [592](#)
FEX (fabric extenders), [24](#), [212–215](#)
FTEP (fabric tunnel endpoint), [60](#), [592](#)
importance of, [42](#)
initialization process
APIC BIOS password, changing, [52](#)
APIC Cisco IMC (Integrated Management Controller) configuration, [52–53](#)
connectivity following switch initialization, [59–62](#)
GIR (Graceful Insertion and Removal), [58](#)
initialization of first APIC, [53–55](#)
initialization of subsequent APICs, [58](#)
switch activation, [55–58](#)
verification of, [59–62](#)
interconnecting with ACI Multi-Site, [557](#)
overview of, [44–45](#)
planning, [45](#), [47–48](#)
APIC connectivity, [46–47](#)
APIC OOB configuration requirements, [47–48](#)
basic configuration parameters, [48–49](#)
cabling requirements, [45](#)
fabric discovery states, [51–52](#)
out-of-band versus in-band management, [48](#)
switch discovery process, [49–51](#)
switch discovery states, [51–52](#)

post-initialization tasks

- automatic upgrades of new switches, 74–75*
- COOP (Council of Oracle Protocol) group configuration, 92*
- default contracts, 64–66*
- DNS (Domain Name System) server configuration, 90–92*
- fabric upgrades, 66–71*
- NTP (Network Time Protocol) synchronization, 84–89*
- pod policy, 83*
- schedulers, 73, 597*
- static out-of-band addresses, assignment of, 63–64*

.aci format, 27

ACI MIB Support List, 502

ACI Multi-Pod

- active/active data center deployments, 562–564
 - overview of, 562–563*
 - stateful-services integration, 563–564*
 - VMM integrations for multiple data centers, 563*
- definition of, 589
- overview of, 15, 25–26
- stateful-services integration, 563–564

ACI Multi-Site, 555–558

- cross-site connectivity, 555–557
- definition of, 589
- extending ACI to remote locations and public clouds, 564
- locally governed configurations, 557

MSO (Multi-Site Orchestrator), [15](#), [27](#), [555](#), [557](#)
MSO-governed configurations, [557](#)
overview of, [15](#), [26-28](#)
primary and disaster recovery data center deployments,
[558-562](#)
*centralized orchestration and management
capabilities*, [559](#)
cross-data center ingress routing optimization, [561](#)
overview of, [558-559](#)
per-bridge domain broadcast and stretch settings, [560](#)
policy deployment to sites, [561](#)
schemas, [557-558](#)
stateful-services integration, [563-564](#)
terminology for, [557](#)

ACI Multi-Tier, [28-30](#)

ACI Virtual Edge (AVE), [24](#), [564](#)
acknowledging faults, [115-116](#)
acquisitions, multitenancy and, [13](#)
activation of switches, [55-58](#)
active controllers, number of, [48](#)
**Active Interval setting (EIGRP Context per Address
Family), [324](#)**

Active state (fabric node discovery), [52](#)

active/active data center deployments, [562-564](#)

overview of, [562-563](#)
stateful-services integration, [563-564](#)
VMM integrations for multiple data centers, [563](#)

adapters, VMkernel, [395](#), [397](#), [405](#), [406](#), [413-414](#)

Adaptive Security Appliance (ASA), 430

Add and Manage Hosts wizard, 411-414

Add vCenter Controller page (vCenter Domain Creation wizard), 409-410

Add VMM Domain Association page, 418

Address Resolution Protocol. See ARP (Address Resolution Protocol)

addresses

- IP (Internet Protocol), 325-326, 470-474, 597
 - dynamic*, 472-474
 - secondary*, 325-326, 597
 - static*, 470-472
- VIP, 245

Admin Distance Preference (OSPF Timer policy), 329

admin role, 520

Admin State parameter

- BGP peer connectivity profiles, 341
- Global MCP Policy, 222

administrative separation, 133

Advertise Subnet option (OSPF), 329

Advertised Externally domain scope, 474-476

advertisement

- of host routes, 321
- of subnets assigned to bridge domains, 314-315

agents, SNMP (Simple Network Management Protocol), 500

agility, network, 8

all security domain, 517

all/aaa/read-all value, 539

all//admin value, 539

all/admin/(16005) value, 539

all/fabric-admin|access-admin/ value, 540

Allow Self AS parameter (BGP peer connectivity profiles), 339

Allowed Self AS Count parameter (BGP peer connectivity profiles), 340

all//read_all value, 539

Amazon Web Services (AWS), 27

Any EPG (vzAny), 364–365, 589

API (application programming interface), 103

APIC (Application Policy Infrastructure Controller) clusters, 9–10, 11

 access policies, 106

 ACI fabric initialization and

APIC Cisco IMC (Integrated Management Controller) configuration, 52–53

BIOS password, changing, 52

connectivity following switch initialization, 59–62

default contracts, 64–66

initialization of first APIC, 53–55

initialization of subsequent APICs, 58

static out-of-band addresses, assignment of, 63–64

verification of, 59–62

 APIC-CLUSTER-L3, 33–34

 APIC-CLUSTER-M3, 33–34

 APIC-CLUSTER-XS, 33–34

CLI (command-line interface), [100-102](#)
 bash shell interactions, [102](#)
 configuration modes, [101](#)
 navigation in, [101](#)
 running configuration, viewing, [102](#)
 vPC (virtual port channel) configuration, [207](#)
components, [46-47](#)
configuration, [47-48](#)
connecting to fabric, [46-48](#)
definition of, [23](#), [589](#)
fabric policies, [106](#)
for in-band management
 access policies for, [468-469](#)
 connectivity preferences, [478-479](#)
scalability and sizing, [33-36](#)
specifications for, [26-28](#)
tenants and, [106](#), [147](#)

APIC OOB Addresses and Default Gateway parameter (ACI fabric initialization), [49](#)

apic#fallback\\username, [549-550](#)

Application Policy Infrastructure Controller. See **APIC (Application Policy Infrastructure Controller) clusters**

application profiles, [527](#)
advantages of, [138-139](#)
configuration, [142-145](#)
definition of, [138](#), [589](#)
multitier application deployment, [264-266](#)

topology, 138–139

application programming interface. *See APIC (Application Policy Infrastructure Controller) clusters*

Application Services Engine (ASE), 27

Application Virtual Switch (AVS), 24

applications, multitier. *See multitier application deployment*

Apply Both Directions feature, 277–278, 476

architecture, ACI (Application Centric Infrastructure), 9–10, 15

ARP (Address Resolution Protocol), 241

- ARP table, 241, 242
- flooding, 262–263, 368
- gleaning, 248–249

ARP Flooding field (bridge domain settings), 369

AS override parameter (BGP peer connectivity profiles), 339

ASA (Adaptive Security Appliance), 430

ASE (Application Services Engine), 27

ASNs (autonomous system numbers), 303, 555

Atomic import mode, 76

attachable access entity profiles. *See AAEPs (attachable access entity profiles)*

Attribute parameter (LDAP providers), 542

audit logs

- definition of, 127, 590
- reviewing, 127–128

authentication. *See AAA (access, authentication, and accounting)*

Authorization Port parameter (RADIUS providers), **540**

Authorization Protocol parameter

RADIUS providers, **540**

TACACS+ providers, **532**

Auto State, L3Out, 299-300

autonomous system numbers (ASNs), **303, 555**

AV pair formatting, **538-540**

AVE (ACI Virtual Edge), **24, 564**

AVS (Application Virtual Switch), **24**

AWS (Amazon Web Services), **27**

B

backups

configuration exports, **75**

configuration imports, **75-76**

configuration rollbacks, **82-83**

configuration snapshots, **80**

importing, **80-82**

on-demand, **76-79**

scheduled, **79-80**

bandwidth, Remote Leaf deployments, **31**

Bandwidth Preference (OSPF Timer policy), **329**

Bandwidth Reference setting (OSPF timer policy), **329**

bare-metal clouds, extending ACI to, 564

Base DN parameter (LDAP providers), 542

bash, 102

BD Multicast Addresses parameter (ACI fabric initialization), 49

BDs (bridge domains)

- advertisement of subnets assigned to, [314–315](#)
- configuration, [142–145](#)
- definition of, [137](#), [590](#)
- DHCP (Dynamic Host Configuration Protocol), [271](#)
- disabling endpoint learning on, [250–251](#)
- extensions, [374–375](#)
- external, [161](#), [380–385](#), [591](#)
- in-band management, [469](#)
- L3Out, [296–298](#), [594](#)
- multitier application deployment, [264–266](#)
- practical application of, [141–142](#)
- service graph settings, [439–440](#)

Beacon Probing, 402

Bell Laboratories, 21

Best Effort import mode, 76

BFD (Bidirectional Forwarding Detection) configuration

- for BGP peering, [339–341](#)
- for EIGRP L3Out, [321–324](#)
- for OSPF L3Outs, [328–329](#)
- switch policies, [174](#)

BFD Interface Profile Creation Wizard, 322-323

BGP (Border Gateway Protocol), 106

ASNs (autonomous system numbers), [303, 555](#)

BGP EVPN router IDs, [556, 590](#)

iBGP peerings, [303-304](#)

L3Out for BGP peering

BFD (Bidirectional Forwarding Detection) implementation, 339-341

BGP timer policies, 338-339, 342

L3Out Creation Wizard, 334-337

node-level customizations, 337-339

OSPF for IP reachability, 343

peer connectivity profiles, 339-341

per-neighbor customizations, 339-341

VRF-level customizations, 342-343

route reflection

definition of, 597

implementation of, 304-305

infra MP-BGP route distribution, 305-306

need for, 303-304

BGP Peer Prefix Policy parameter (BGP peer connectivity profiles), 341

Bidirectional Forwarding Detection. See [BFD \(Bidirectional Forwarding Detection\) configuration](#)

Bidirectional Forwarding Detection parameter (BGP peer connectivity profiles), 340

Bind DN parameter (LDAP providers), 542

binding

dynamic, 159
static, 159

bindings, port, 400, 596

BIOS password, changing, 52

Blacklist port usage, 195

blacklisting, 14, 318-320, 590

bocks, port, 198-199

Border Gateway Protocol. See **BGP (Border Gateway Protocol)**

border leaf switches, 24, 590

bounce entry, 247

BPDUs (bridge protocol data units), 386-388

- BPDU Filter, 230-231
- BPDU Guard, 230-231
- PVST+ (Per-VLAN Spanning Tree), 387-388
- Rapid PVST+ (Rapid Per-VLAN Spanning Tree), 387-388
- TCNs (topology change notifications), 386-387

bridge domains. See **BDs (bridge domains)**

bridge protocol data units. See **BPDUs (bridge protocol data units)**

bridge-domain BD-CRITICAL-STUFF command, 147

broadcast, unknown unicast, and multicast forwarding. See **BUM (broadcast, unknown unicast, and multicast) forwarding**

broadcast settings, 560

Broadcom, 103

BUM (broadcast, unknown unicast, and multicast) forwarding, 25, 223

ingress replication of, 28
preventing, 560
storm control, 223-224

C

cabling, ACI fabric initialization, 45
CAM (content-addressable memory), 362
cat /etc/ntp.conf command, 86-87
CDP (Cisco Discovery Protocol)
 configuration, 190
 interface policies, 171
centralized organization, 559
channels, port. See [port channels](#)
Cisco Adaptive Security Appliance (ASA), 430
Cisco Application Services Engine (ASE), 27
Cisco AV pair formatting, 538-540
Cisco Cloud APIC, 564
Cisco Cloud Service Router (CSR) 1000V, 564
Cisco FabricPath, 7
Cisco Firepower Management Center (FMC), 432
Cisco IMC (Integrated Management Controller), 52-53, 100, 589
Cisco Nexus 1000v distributed virtual switch, 9
Cisco Overlay Transport Virtualization (OTV), 560
Cisco Tetration, 272
Cisco Unified Computing System (UCS), 218

Citrix NetScaler Management and Analytics System (MAS), 432

Class of Service (CoS), 218

classes, 590

- aaaSessionLR, 128
- definition of, 109
- faultDelegate, 116-118
- faultInst, 116-118
- monCommonPol, 118
- monEPGPol, 118
- monFabricPol, 118
- monInfraPol, 118

Cleared faults, 112

Clearing Interval timer, 115

CLIs (command-line interfaces)

- APIC CLI, 100-102
 - bash shell interactions, 102*
 - configuration modes, 101*
 - navigation in, 101*
 - running configuration, viewing, 102*
 - tenant object configuration, 147*
 - vPC (virtual port channel) configuration, 207*
- overview of, 100
- switch CLI, 102-103

Clos, Charles, 21

Clos topology, 21-22

Cloud APIC, 564

Cloud Service Router (CSR) 1000V, 564

CloudSec encryption, 556, 590

clusters, APIC. See [APIC \(Application Policy Infrastructure Controller\) clusters](#)

clusters, MSO (Multi-Site Orchestrator), 555

CNA (converged network adapters), 218

commands. See *individual commands*

common security domain, 517

common tenants, 135

common//read-all value, 540

Communication faults, 113

components. See [hardware components](#)

compute leaf switches, 24, 590

concrete devices, 444, 449-450, 590

configuration backups, importing, 80-82

configuration exports, 75

Configuration faults, 113

configuration imports, 75-76

configuration rollbacks, 82-83

configuration snapshots, 80

configure command, 101

Configure Interface, PC, and VPC Wizard, 211-212

configure terminal command, 101

Confirm New Password dialog box, 52

conformity, template, 557, 599

Console Authentication Realm setting (AAA policy), 549

constructs, ACI Multi-Site, 557

consumers, 149–150, 590

content-addressable memory (CAM), 362

contexts, SNMP (Simple Network Management Protocol), 506

contexts, VRF. See [VRF \(virtual routing and forwarding\) instances](#)

contracts, 148–151

- ACI fabric initialization, [64–66](#)
- Apply Both Directions feature, [277–278](#)
- assigning to EPGs, [278–279](#)
- definition of, [148–149, 590](#)
- direction of, [149–150](#)
- filters, [148–149, 592](#)
 - for bidirectional application, 273–275*
 - for unidirectional application, 280*
- L3Out for EIGRP peering, [316–318](#)
- for out-of-band (OOB) management, [479–480](#)
- overview of, [272](#)
- planning, [272–273](#)
- Reverse Filter Ports feature, [277–278](#)
- scope of, [150–151, 284–285, 590](#)
- service graphs, [427–428](#)
- SNMP (Network Management Protocol), [503](#)
- Stateful feature, [284](#)
- subjects, [278](#)
 - for bidirectional application, 275–276*

definition of, [148-149](#)
for unidirectional application, [280-281](#)
verification of, [278](#)
syslog forwarding, [487-491](#)
TCP established session rule, [279-280](#)
verifying enforcement of, [283-284](#)
VRF-level enforcement, [367](#)
whitelisting, [282-283](#)
zero-trust networks and, [151](#)

Control Plane Policing (CoPP)

configuration, [225-229](#)
switch policies, [174](#)

controller ID parameter (ACI fabric initialization), [49](#)

controller name parameter (ACI fabric initialization), [49](#)

Controller port usage, [195](#)

controller role, [57](#)

converged network adapters (CNA), [218](#)

COOP (Council of Oracle Protocol), [23, 62, 92, 243](#)

Coordinated Universal Time (UTC), [89](#)

CoPP (Control Plane Policing)

configuration, [225-229](#)
interface policies, [172](#)
prefilter switch policies, [175](#)
switch policies, [174](#)

CoS (Class of Service), [218](#)

Council of Oracle Protocol. See [COOP \(Council of Oracle Protocol\)](#)

Create Access Port Selector, [191](#)

Create Application EPG wizard, [265-266](#)

Create Application Profile wizard, [144-146](#)

Create Bridge Domain wizard, [142-144, 264-265](#)

Create Bridged Outside wizard, [380-385](#)

Create Configuration Export Policy wizard, [76-78, 80-81](#)

Create Contract page, [275](#)

Create Contract Subject page, [275-276](#)

Create Date and Time Policy window, [85](#)

Create DHCP Relay Label wizard, [271](#)

Create DNS Profile option, [90](#)

Create External Management Network Instance Profiles command, [64-65, 491](#)

Create Filter wizard, [488](#)

Create LDAP Group Map Rules wizard, [543-547](#)

Create LDAP Provider wizard, [543](#)

Create Leaf Breakout Port Group page, [216](#)

Create Leaf Interface Profile wizard, [179-180](#)

Create Leaf Profile wizard, [180-181](#)

Create Local User wizard, [521-523](#)

Create Login Domain page, [535](#)

Create New Password dialog box, [52](#)

Create Out-of-Band Contract page, [489](#)

Create Physical Domain wizard, [163](#)

Create RBAC Rule wizard, [529-531](#)

Create Remote Location wizard, 77

Create Role page, 520

Create Security Domain window, 517

Create SNMP Monitoring Destination Group command, 507

Create Static Node Management Addresses page, 63, 470-471

Create Syslog Monitoring Destination Group command, 492

Create Syslog Source wizard, 494-495

Create Tenant wizard, 133-134

Create vCenter Credential page (vCenter Domain Creation wizard), 409

Create vCenter Domain page (vCenter Domain Creation wizard), 409, 410

Create VLAN Pool wizard, 159-160

Create VPC Explicit Protection Group wizard, 202-203

Create VRF wizard, 135-137

Critical faults, 112

cross-fabric namespace normalization, 28

cross-platform integrations, 15

cross-site connectivity, 555-557

CSR (Cloud Service Router) 1000V, 564

Custom EPG Name field, 416

Custom Filter parameter (LDAP providers), 542

custom function profiles, 444-445

custom RBAC (role-based access control) rules, 528-531

D

data center deployments

with ACI Multi-Site, [558–562](#)

active/active data centers, [562–564](#)

overview of, [562–563](#)

stateful-services integration, [563–564](#)

VMM integrations for multiple data centers, [563](#)

extension and migration, Remote Leaf deployments for,
[30](#)

multitenancy, [12–13](#)

primary and disaster recovery data centers, [558–562](#)

centralized orchestration and management capabilities, [559](#)

cross-data center ingress routing optimization, [561](#)

overview of, [558–559](#)

per-bridge domain broadcast and stretch settings, [560](#)

traditional networks

agility of, [8](#)

management of, [4–5](#)

scalability and growth of, [5–7](#)

security of, [8–9](#)

three-tier design of, [5–7](#)

visibility of, [9](#)

data plane policing (DPP), [172](#)

database sharding, [34–35](#), [597–598](#)

date/time, NTP (Network Time Protocol) synchronization, [84–89](#), [106](#)

Datetime Format object, 89

DCACI 300-620 exam

final review/study, 570

preparation for, 566-570

Pearson IT Certification test prep software, 567-570

tips and guidelines, 566-567

updates to, 586-587

DCACIA 300-630 exam, 361

Default Authentication Realm setting (AAA policy), 548

Default Firmware Version setting, 74-75

delimiter characters, 416

demilitarized zone (DMZ), 8

deployment immediacy, 268, 405-407, 590

design, VLAN pools and domains, 161-163

hybrid approach, 162-163

single VLAN pool for each type of domain, 161

single VLAN pool per function, 162

destination groups

SNMP (Simple Network Management Protocol), 507-508

syslog monitoring, 492-493

Development/tenant-admin/ value, 540

device managers, 433-434, 590

device packages, importing, 430, 441-442

device selection policies, 446

devices, deploying service graphs for

devices in GoThrough Mode, 436, 437

devices in GoTo Mode, 435, 436–437

one-arm load balancers, 437

DHCP (Dynamic Host Configuration Protocol) relay, 32, 219–221, 271

DHT (distributed hash table), 92

Differentiated Services Code Point (DSCP), 218

direction, of contracts, 149–150

Disable Connected Check parameter (BGP peer connectivity profiles), 340

Disable Peer AS Check parameter (BGP peer connectivity profiles), 340

Disabled/Decommissioned state (fabric node discovery), 52

disabling

contract enforcement at VRF instance level, 367

endpoint learning

on bridge domain, 250–251

at VRF level, 251

disaster recovery (DR)

data center deployments with ACI Multi-Site, 558–562

centralized orchestration and management capabilities, 559

cross-data center ingress routing optimization, 561–562

overview of, 558–559

per-bridge domain broadcast and stretch settings, 560

Remote Leaf deployments, 31

Discovering state (fabric node discovery), 52

Discovery port usage, 195

discovery process, ACI fabric initialization

- fabric discovery stages, 51
- switch discovery and activation, 55–58
- switch discovery process, 49–51
- switch discovery states, 51–52

distinguished names (DNs), 109, 591

distributed hash table (DHT), 92

distributed port groups, 397

- assigning VMs (virtual machines) to, 417–418
- pushing EPGs (endpoint groups) to vCenter as, 415–416

Distributed Resource Scheduler (DRS), 399

DMZ (demilitarized zone), 8

DNs (distinguished names), 109, 591

DNS (Domain Name System), 90–92, 106

dns command, 101

Domain Name System. See DNS (Domain Name System)

domain profiles (VMM), 408–410

domains

- assigning to EPGs, 267
- associating VLAN pools with, 163–164
- BDs (bridge domains)
 - advertisement of subnets assigned to, 314–315*
 - configuration, 142–145*
 - definition of, 137*
- DHCP (Dynamic Host Configuration Protocol), 271*

external, [161](#), [591](#)
L3Out, [296-298](#), [594](#)
multitier application deployment, [264-266](#)
practical application of, [141-142](#)

creating, [163](#)
definition of, [591](#)
designs for, [161-163](#)
 hybrid approach, [162-163](#)
 single VLAN pool for each type of domain, [161](#)
 single VLAN pool per function, [162](#)

external bridged, [380-385](#)
external routed, [161](#), [591](#)
fallback, [549-550](#)
fault, [113](#)
Fibre Channel, [161](#)
L3 domain implementation examples, [301-302](#)
mapping to security domain, [526-528](#)
physical, [161](#), [595](#)
security, [517-518](#)
 assigning tenants to, [517-518](#)
 creating, [517](#)
 definition of, [517](#), [597](#)
 mapping domains to, [526-528](#)
 predefined, [517](#)

types of, [160-161](#)
UCS (Unified Computing System) domains, [218](#)
VMM (Virtual Machine Manager), [161](#), [418](#), [599](#)

vPC (virtual port channel) domain, 201-204

DPP (data plane policing), 172

DR. See [disaster recovery \(DR\)](#)

Drop option (Multi Destination Flooding), 370

DRS (Distributed Resource Scheduler), 399

DSCP (Differentiated Services Code Point), 218

DTEP (dynamic tunnel endpoint), 61, 591

DWDM, 173

dynamic breakout ports, 215-217, 591

dynamic endpoint attach, 439

Dynamic Host Configuration Protocol. See [DHCP \(Dynamic Host Configuration Protocol\) relay](#)

dynamic IP addressing, 472-474

dynamic port bindings, 400

dynamic tunnel endpoint (DTEP), 61, 591

dynamic VLAN allocation, 159, 591

E

east-west traffic, 7

eBGP Distance parameter (BGP timer policy), 342

eBGP/iBGP Max ECMP parameter (BGP timer policy), 342

ECMP (equal-cost multipathing), 325

EDT (Error Detect Timeout), 175

EIGRP (Enhanced Interior Gateway Routing Protocol) peering, L3Out configuration for, 305-306, 324-325

advertisement of host routes, 321

advertisement of subnets assigned to bridge domains, [314-315](#)

authentication, [324](#)

BFD (Bidirectional Forwarding Detection) implementation, [321-324](#)

blacklist EPG (endpoint group) with logging, [318-320](#)

contracts, [316-318](#)

EIGRP Context per Address Family, [324-325](#)

external EPG (endpoint group) deployment, [310-312](#)

forwarding verification, [312-314](#)

L3Out Creation Wizard, [307-309](#)

route advertisement, [328](#)

VRF-level customizations, [324-325](#)

electronic programmable logic device (EPLD) upgrades, [66](#)

Enable Host Route Leak parameter (BGP timer policy), [342](#)

Enable MCP PDU Per VLAN setting (Global MCP Policy), [222](#)

Enable Name Lookup for Router IDs setting (OSPF timer policy), [329](#)

Enable SSL parameter (LDAP providers), [542](#)

Encap Scope, L3Out, [298-299](#)

encapsulation, port, [246](#)

encryption, CloudSec, [556, 590](#)

end command, [101](#)

endpoint groups. See [EPGs \(endpoint groups\)](#)

endpoint learning. See also [endpoints; EPGs \(endpoint groups\)](#)

definition of, [591](#)

disabling

on bridge domain, [250-251](#)

at VRF level, [251](#)

endpoint movements within ACI fabric, [247](#)

Enforce Subnet Check feature, [250](#)

hardware proxy, [247-248](#)

on L3Outs, [249](#)

Limit IP Learning to Subnet feature, [249-250](#)

local versus remote endpoints, [242-243](#), [594](#), [596](#)

lookup tables, [241-242](#)

network migrations into ACI, [371-372](#)

overview of, [241](#)

remote, [244-245](#)

for silent hosts, [245-247](#)

spine proxy, [247-248](#)

unicast routing and, [243-244](#)

VLAN IDs, [245-247](#), [253-254](#)

VNIDs (VXLAN network identifiers), [244](#), [245-247](#)

endpoints. *See also endpoint learning; EPGs (endpoint groups)*

definition of, [591](#)

dynamic endpoint attach, [439](#)

endpoint tables, [242](#)

local versus remote, [242-243](#), [594](#), [596](#)

local versus remote endpoints, [596](#)

movements within ACI fabric, [247](#)

number of, [4](#)

TEPs (tunnel endpoints)

- overlay multicast*, [555](#), [595](#)
- overlay unicast*, [555](#), [595](#)
- PTEP (physical tunnel endpoint)*, [60](#), [595](#)
- TEP pools*, [49](#), [50](#), [57](#), [59](#), [599](#)
- verifying addresses of*, [60-62](#)

verification of traffic path between, [254-256](#)

Enforce Bootscript Version Validation setting, [74](#)

Enforce Subnet Check feature, [250](#)

Enhanced Interior Gateway Routing Protocol. See
[EIGRP \(Enhanced Interior Gateway Routing Protocol\) peering](#), [L3Out configuration for enhanced LACP policy support](#), [419-421](#)

Enter Password dialog box, [52](#)

Environmental faults, [113](#)

EPG-Login-Servers, [384](#)

EPGs (endpoint groups), [151-153](#)

- AAEP (attachable access entity profile) configuration, [207-210](#)
- Any EPG (vzAny), [364-365](#), [589](#)
- blacklist EPG with logging, [318-320](#)
- classifying endpoints into, [146-147](#)
- configuration, [142-145](#)
- contracts, assigning to, [278-279](#)
- definition of, [137-138](#)
- domains, assigning to, [267](#)
- extensions

bridge domain extensions compared to, 374–375
definition of, 372–373, 375–380

external, 151–153, 294, 310–312, 591
in-band management, 470–471, 476–477
for multitier application deployment
 DHCP (Dynamic Host Configuration Protocol) relay, 271
 EPG configuration, 264–266
 EPG mapping to ports, 267–269, 270
 policy deployment, 270
 verification of EPG-to-port assignments, 269–270
out-of-band (OOB) management, 480, 491
port usage, 195
practical application of, 141–142
pushing to vCenter as distributed port groups, 415–416
shadow, 428–429, 597

ephemeral port bindings, 400

EPLD (electronic programmable logic device) upgrades, 66

equal-cost multipathing (ECMP), 325

equipment flash configuration policies, 176

Error Detect Timeout (EDT), 175

Error Disabled Recovery Policy, 231–232

established session rule (TCP), 279–280

ESXi

servers
 adding to VDS (vSphere distributed switches), 411–414
 connecting in UCS domains, 407

connecting to fabric, 407
definition of, 395
standard switch architecture, 395
VMkernel interface, 397–399
vSphere distributed switches (VDS), 397

VMs (virtual machines), 27

Ethernet ports, 46

events

definition of, 126
event records, 591
squelching, 127, 598
viewing, 126

exam, DCACI 300-620

final review/study, 570
preparation for, 566–570
Pearson IT Certification test prep software, 567–570
tips and guidelines, 566–567
updates to, 586–587

exports, configuring, 75

Extensible Markup Language (XML), 103

extension, Layer 2. *See also BDs (bridge domains); EPGs (endpoint groups)*

ACI interaction with STP (Spanning Tree Protocol), 386–388
link types, 388
MCP (MisCabling Protocol), 388
MST (Multiple Spanning Tree) instance mappings, 387–388

TCNs (topology change notifications), [386–387](#)

Layer 2 connectivity to non-ACI switches

bridge domain extensions, [374–375](#)

EPG (endpoint group) extensions, [372–373, 375–380](#)

L2Outs, [380–385](#)

migration of overlapping VLANs into ACI, [385–386](#)

overview of, [372](#)

network migrations into ACI

Any EPG (vzAny), [364–365, 589](#)

contract enforcement at VRF instance level, [367](#)

endpoint learning considerations, [371–372](#)

flooding requirements, [368–370](#)

full-mesh network-centric contracts, [362–364](#)

GARP-based detection, [370–371](#)

Legacy mode, [371](#)

network-centric deployments, [361–362](#)

overview of, [361](#)

preferred group members, [365–367](#)

preparation for, [372](#)

security enforcement in, [362](#)

overview of, [358](#)

external (L3Out) bridge domains, [296–298](#)

external AAA server integration, [532](#)

AAA authentication policy settings, [547–550](#)

configuration options, [548–549](#)

fallback domain, [550](#)

login domains and global AAA settings, [549–550](#)

ACI configuration for LDAP, [541–547](#)
 configuration parameters, [541–543](#)
 Create LDAP Group Map Rules wizard, [543–547](#)
 Create LDAP Provider wizard, [543](#)

ACI configuration for RADIUS, [540–541](#)

ACI configuration for TACACS+, [532–536](#)

Cisco AV pair formatting, [538–540](#)

ISE (Identity Service Engine) configuration, [536–538](#)

external advertisement, inb bridge domain, [474–476](#)

external BDs (bridge domains), [591](#)

external bridge domains, [161](#), [380–385](#)

external bridged networks, [372](#), [375](#), [380](#), [591](#)

External Distance setting (EIGRP Context per Address Family), [325](#)

External EPG Creation Wizard, [310–312](#)

External EPG Networks page (Create Bridged Outside wizard), [382](#)

external EPGs (endpoint groups), [151–153](#), [294](#), [310–312](#), [591](#)

External Management Network Instance Profile folder, [64–65](#)

external management network instance profiles, [491](#)

external routed domains, [161](#), [591](#)

external VLAN ranges, [160](#)

F

Fabric Connectivity Infra page, [556](#)

fabric extenders (FEX), 212-215

Fabric External port usage, 195

fabric ID parameter (ACI fabric initialization), 48

fabric initialization. See ACI fabric initialization

Fabric Membership view, 57-58

fabric name parameter (ACI fabric initialization), 48

fabric policies, 106, 592

fabric ports, 23, 195, 592

fabric tunnel endpoint (FTEP), 592

fabric-admin role, 520

fabric-equipment privilege, 519

FabricPath, 7

Failover Order setting, 403

failover policies, 400-403

Fallback Check setting (AAA policy), 549

fallback domain, 549-550

Fallback setting, 403

Fast Select Hot Standby Ports setting, 196, 201

fault domains, 13-14

Fault Severity Assignment Policies folder, 122

faultDelegate class, 116-118

faultInst class, 116-118

faults

- acknowledging, 115-116
- definition of, 592
- domains, 113
- fault management policies, 120-121

fault MOs, [116–118](#)
isolation of, [133](#)
lifecycle, [113–115](#), [592](#)
phases, [114–115](#)
timers, [115](#)
overview of, [111](#)
policies, [120–121](#)
severity levels, [111–112](#), [121–124](#)
types of, [113](#)
viewing, [111](#)

FC port channel interface policy groups, [171](#)

FEX (fabric extenders), [24](#), [212–215](#)

FHRP (first-hop redundancy protocol), [6](#)

Fibre Channel (FC), [172](#)

domains, [161](#)
interface policy groups, [171](#)
switch policies, [175](#)

Filter Type parameter (LDAP providers), [542](#)

filters

creating
for bidirectional application, [273–275](#)
for unidirectional application, [280](#)
definition of, [148–149](#), [592](#)
filter entries, [148](#)
in-band management, [476–477](#)
Stateful feature, [284](#)
for syslog forwarding, [487–491](#)

finite state machine (FSM), [111](#)

Firepower Management Center (FMC), [432](#)

firewall-domain, [162](#), [164](#)

firewalls

- interface policies, [173](#)
- service graphs
 - for managed devices,* [453-460](#)
 - unmanaged firewall pair deployment,* [447-452](#)

first-generation leaf switches, [38-39](#)

first-generation spine switches, [37](#)

first-hop redundancy protocol (FHRP), [6](#)

Flash Card mode, Pearson IT Certification test prep software, [568-569](#)

floating SVIs (switch virtual interfaces), [296](#), [592](#)

Flood in BD option (Multi Destination Flooding), [370](#)

Flood in Encapsulation option (Multi Destination Flooding), [370](#)

flooding, [368-370](#)

- ARP (Address Resolution Protocol), [262-263](#), [369](#)
- Forwarding setting, [368](#)
- L2 Unknown Unicast, [368](#)
- L3 Unknown Multicast, [369](#)
- Multi Destination, [370](#)

flow control, PFC (priority-based flow control), [172](#)

FMC (Firepower Management Center), [432](#)

folded Clos topology, [21-22](#)

forwarding, [62](#)

L3Out for EIGRP peering, [312-314](#)
packet, [251](#)
both endpoints attach to same leaf, [251-254](#)
flooding to unknown destination, [261-263](#)
known destination behind another leaf, [254-258](#)
spine proxy to unknown destination, [258-261](#)
system messages to syslog servers
contracts for, [487-491](#)
steps for, [487](#)
syslog monitoring destination groups, [492-493](#)
syslog sources, [494-498](#)
verification of, [498-500](#)

Forwarding field (bridge domain settings), [368](#)
forwarding scale profiles, [175](#)
forwarding tag trees. See [FTag trees](#)
FQDNs (fully qualified domain names), [126](#)
FSM (finite state machine), [111](#)
FTag topology, [261-262](#)
FTag trees, [261, 262, 592](#)
FTEP (fabric tunnel endpoint), [60, 592](#)
full-mesh network-centric contracts, [362-364](#)
fully qualified domain names (FQDNs), [126](#)
function nodes, [445-446](#)
function profiles
 creating custom, [444-445](#)
 definition of, [592](#)
 examples of, [430-433, 442](#)

functions, service graphs as concatenation of, 427-428

G

GARP (Gratuitous ARP), 241, 370-371

gateways

- for in-band management, 469-470
- pervasive, 252-254, 595

Gigabit Ethernet dedicated management ports, 46

GIR (Graceful Insertion and Removal), 58

Global AES Encryption Settings for All Configuration Import and Export page, 78

global MIB (Management Information Base) scope, 502, 592

GoThrough mode, devices in, 436, 437

GoTo mode, devices in, 435, 436-437

Graceful Convergence setting, 196, 201

Graceful Insertion and Removal (GIR), 58

Graceful Restart Helper setting

- BGP timer policy, 338
- OSPF timer policy, 329

granting access, 523-525

graphical user interface. See GUI (graphical user interface)

graphs, service. See service graphs

Gratuitous ARP (GARP), 241, 370-371

grep command, 102

GUI (graphical user interface), 99, 107-108

H

hardware components. *See APIC (Application Policy Infrastructure Controller) clusters; switches*

hardware proxy, 247-248

hardware proxy forwarding, 62

hashes, 402

headend replication (HER) tunnels, 32

health monitoring, 16

audit logs

definition of, 127

reviewing, 127-128

events

definition of, 126

event records, 126

squelching, 127, 598

viewing, 126

faults

acknowledging, 115-116

definition of, 592

domains, 113

fault management policies, 120-121

fault MOs, 116-118

lifecycle, 113-115, 592

overview of, 111

severity levels, 111-112, 121-124

squelching, [121-124](#)

types of, [113](#)

viewing, [111](#)

health scores, [122-125, 592-593](#)

overview of, [110-111](#)

policies for, [118-120](#)

Health Score Evaluation policy, 125

health scores, 122-125, 592-593

HER (headend replication) tunnels, 32

hierarchy

access policies, [183-184](#)

tenant, [153-154](#)

Hold Interval (BGP timer policy), 338

Host Name parameter

LDAP providers, [542](#)

RADIUS providers, [540](#)

TACACS+ providers, [532](#)

host routes, advertisement of, 321

hosts

ESXi

adding to VDS (vSphere distributed switches), [411-414](#)

connecting in UCS domains, [407](#)

connecting to fabric, [407](#)

definition of, [395](#)

standard switch architecture, [395](#)

VMkernel interface, [397-399](#)

vSphere distributed switches (VDS), [397](#)

silent, 245–247, 248–249

HSRP (Hot Standby Router Protocol), 344

HTTP (Hypertext Transfer Protocol), 67

hybrid mode, service graph deployment, 428, 432–434

I

iBGP Distance parameter (BGP timer policy), 342

iBGP peerings, 303–304

Identity Service Engine (ISE), 536–538

IDs

BGP EVPN router, 556, 590

node, 11, 595

VLAN, 245–247, 253–254

VNIDs, 244, 245–247

IEEE (Institute of Electrical and Electronics Engineers) 802.1Q standard, 7

IFM (intra-fabric messaging), 50–51, 593

IGMP (Internet Group Management Protocol) snooping, 368

Ignore Fault window, 122

IMC (Integrated Management Controller), 52–53, 100

immediacy settings, VMM (Virtual Machine Manager), 405–407

Import Mode parameter, 75

Import Type parameter, 75

imports

ACI Multi-Site, [557](#)

configuration backups, [80-82](#)

configuration imports, [75-76](#)

device packages, [430, 441-444](#)

Inactive state (fabric node discovery), [52](#)

in-band management, [462](#)

configuration

access policies for APIC in-band interfaces, [468-469](#)

APIC connectivity preferences, [478-479](#)

bridge domains, [469](#)

in-band network, extending out of fabric, [474-476](#)

IP addressing, [470-474](#)

steps for, [467-468](#)

whitelisting desired connectivity to/from, [476-477](#)

connectivity, [465-467](#)

deployment alongside out-of-band (OOB) management,
[467](#)

out-of-bank (OOB) management compared to, [48](#)

inbound route filtering, [352-353](#)

Info faults, [112](#)

informs, SNMP (Simple Network Management Protocol), [501](#)

infra IP reachability, [32](#)

Infra port usage, [195](#)

infra tenants, [134-135, 292](#)

infrastructure VLAN, [49, 593](#)

ingress replication, [28](#)

ingress routing optimization

cross-data center ingress routing optimization, [561–562](#)

primary and disaster recovery data center deployments,
[561](#)

Initial Delay setting (Global MCP Policy), [222](#)

initialization of ACI fabric. *See* [ACI fabric initialization](#)

Institute of Electrical and Electronics Engineers 802.1Q standard, [7](#)

integrated health monitoring. *See* [health monitoring](#)

Integrated Management Controller. *See* [IMC \(Integrated Management Controller\)](#)

interface bridge-domain BD-CRITICAL-STUFF command, [147](#)

interface policies, [169–174](#)

CDP (Cisco Discovery Protocol), [190](#)

definition of, [593](#)

deployment of, [173–174](#)

EIGRP (Enhanced Interior Gateway Routing Protocol), [321–323](#)

link level, [189](#)

LLDP (Link Layer Discovery Protocol), [189](#)

OSPF (Open Shortest Path First), [326–327](#)

overview of, [169–170](#)

port channel, [198](#)

Storm Control, [223–224](#)

types of, [170–173](#)

vPC (virtual port channel), [205–206](#)

interface policy groups, [169–174](#)

definition of, 593

overview of, 169–170

types of, 170–171

interface profiles, 179, 294

configuration, 179–182

definition of, 593

logical, 295, 594

interface selectors, 179, 593

interleak, 305, 593

Intermediate System-to-Intermediate System (IS-IS), 23, 60, 106

Internal Distance setting (EIGRP Context per Address Family), 325

internal VLAN ranges, 160

Internet Group Management Protocol (IGMP) snooping, 368

interpod network (IPN), 25

intersite L3Out, 557, 593

intersite networks. See ISNs (intersite networks), ACI Multi-Site

intra-fabric messaging (IFM), 50–51, 593

IP (Internet Protocol)

addresses, 470–474

dynamic, 472–474

secondary, 325–326, 597

static, 470–472

IP hash, routes based on, 402

IP storage leaf switches, 24, 593

IPv6, 241, 344

service-level agreement (SLA) tracking, 330–334

ip address command, 147

IP Address parameter

LDAP providers, 542

RADIUS providers, 540

TACACS+ providers, 532

IP storage leaf switches, 24, 593

IPN (interpod network), 25

ISE (Identity Service Engine), 536–538

IS-IS (Intermediate System-to-Intermediate System), 23, 60, 106

ISNs (intersite networks), ACI Multi-Site, 27, 555–558

cross-site connectivity, 555–557

extending ACI to remote locations and public clouds, 564

locally governed configurations, 557

MSO-governed configurations, 557

primary and disaster recovery data center deployments,
558–562

schemas, 557–558

stateful-services integration, 563–564

terminology for, 557

ITSM (IT service management), 110

J-K

JavaScript Object Notation (JSON), 103

JSON (JavaScript Object Notation), 103

Keepalive Interval (BGP timer policy), 338

Key parameter

Global MCP Policy, 222

RADIUS providers, 540

TACACS+ providers, 532

keychain policy, 324

KVM (Keyboard Video Mouse), 100

L

L2 interface policy, 172

L2 Unknown Unicast field (bridge domain settings), 368, 593

L2Outs, 380-385

L3 APIC (Application Policy Infrastructure Controller) specifications, 33

L3 domain implementation, 301-302

L3 Unknown Multicast Flooding field (bridge domain settings), 369

L3Out Creation Wizard

AAEPs (attachable access entity profiles), 302

configuration for BGP peering, 334-337

configuration for EIGRP peering, 307-309

configuration for OSPF peering, 325-327

L3Outs, 153, 284

anatomy of, 293-295

configuration for BGP peering

BFD (Bidirectional Forwarding Detection) implementation, [339-341](#)

BGP timer policies, [338-339](#), [342](#)

L3Out Creation Wizard, [334-337](#)

node-level customizations, [337-339](#)

OSPF for IP reachability, [343](#)

peer connectivity profiles, [339-341](#)

per-neighbor customizations, [339-341](#)

VRF-level customizations, [342-343](#)

configuration for EIGRP peering, [305-306](#)

advertisement of host routes, [321](#)

advertisement of subnets assigned to bridge domains, [314-315](#)

authentication, [324](#)

BFD (Bidirectional Forwarding Detection) implementation, [321-324](#)

blacklist EPG (endpoint group) with logging, [318-320](#)

contracts, [316-318](#)

EIGRP Context per Address Family, [324-325](#)

external EPG (endpoint group) deployment, [310-312](#)

forwarding verification, [312-314](#)

L3Out Creation Wizard, [307-309](#)

route advertisement, [328](#)

VRF-level customizations, [324-325](#)

configuration for OSPF peering, [329](#)

BFD (Bidirectional Forwarding Detection) implementation, [328-329](#)

L3Out Creation Wizard, [325-327](#)

OSPFv3 support, [344](#)
route advertisement, [328](#)
VRF-level customizations, [329](#)

definition of, [593–594](#)
endpoint learning on, [249](#)
HSRP (Hot Standby Router Protocol), [344](#)
interface types, [296](#)
intersite, [557](#), [593](#)
IPv6 and, [344](#)
key functions of, [293](#)
L3Out BDs (bridge domains), [296–298](#), [594](#)
logical node and interface profiles, [295](#), [594](#)
node and interface profiles, [294](#)
prerequisites for
 BGP (Border Gateway Protocol) route reflection, [303–305](#), [597](#)
 infra MP-BGP route distribution, [305–306](#)
 L3 domain implementation examples, [301–302](#)
 overview of, [301](#)
route control
 inbound route filtering, [352–353](#)
 overview of, [344–345](#)
 policies for, [351–352](#)
 route attributes to all peers, [346–349](#)
 route attributes to specific peer, [349–351](#)
 route profiles, [344–345](#), [597](#)
static routes on

IP service-level agreement (SLA) tracking, [330–334](#)
overview of, [329–330](#)

stub network and transit routing, [291–292](#)

SVI Auto State, [299–300](#)

SVI Encap Scope, [298–299](#)

types of, [292–293](#)

VLAN pool assignment, [301–302](#)

L4-L7 devices, identifying to fabric, [443–444](#)

L4-L7 services, [106, 435–436](#)

LACP (Link Aggregation Control Protocol), [202, 419–421](#)

LAN on motherboard (LOM) ports, [47](#)

latency, Remote Leaf deployments, [31](#)

Layer 2 extension to non-ACI switches

ACI interaction with STP (Spanning Tree Protocol), [386–388](#)

link types, [388](#)

MCP (MisCabling Protocol), [388](#)

MST (Multiple Spanning Tree) instance mappings, [387–388](#)

TCNs (topology change notifications), [386–387](#)

Layer 2 connectivity to non-ACI switches

bridge domain extensions, [374–375](#)

EPG (endpoint group) extensions, [372–373, 375–380](#)

L2Outs, [380–385](#)

migration of overlapping VLANs into ACI, [385–386](#)

overview of, [372](#)

network migrations into ACI

Any EPG (vzAny), 364–365, 589
contract enforcement at VRF instance level, 367
endpoint learning considerations, 371–372
flooding requirements, 368–370
full-mesh network-centric contracts, 362–364
GARP-based detection, 370–371
Legacy mode, 371
network-centric deployments, 361–362
overview of, 361
preferred group members, 365–367
preparation for, 372
security enforcement in, 362
overview of, 358

Layer 3 Outside. See [L3Outs](#)

LDAP (Lightweight Directory Access Protocol)

ACI configuration for, 541–547
Create LDAP Group Map Rules wizard, 543–547
Create LDAP Provider wizard, 543

leaf access port policy groups, 170, 191

leaf breakout port groups, 171

leaf interface override policy, 232, 594

leaf selectors, 181

leaf switches, 9–10

border, 24, 590
cabling requirements, 45
compute, 24, 590
definition of, 22, 594

first-generation, 38–39
initialization of, 51
IP storage, 24, 593
leaf access port policy groups, 191
overview of, 23
packet forwarding scenarios, 251
both endpoints attach to same leaf, 251–254
flooding to unknown destination, 261–263
known destination behind another leaf, 254–258
spine proxy to unknown destination, 258–261
pervasive gateways, 252–254, 595
pervasive routes, 258–260, 595
profiles, 179–182
purchasing decisions, 38
second-generation, 39–40
service, 24, 597
transit, 25, 599

leaf topologies. *See* **topologies**

leaking, route, 466

learning, endpoint. *See* **endpoint learning**

Legacy mode, 371

Lightweight Directory Access Protocol. *See* **LDAP (Lightweight Directory Access Protocol)**

Limit IP Learning to Subnet feature, 249–250

Link Aggregation Control Protocol (LACP), 202

link debounce interval, 189, 594

Link Layer Discovery Protocol. See [LLDP \(Link Layer Discovery Protocol\)](#)

link level interface policies, [171, 189](#)

Link Status Only option, [402](#)

links, STP (Spanning Tree Protocol), [388](#)

LLDP (Link Layer Discovery Protocol)

 interface policies, [171, 189](#)

 neighbor discovery, [50](#)

load balancing, [600](#)

 one-arm load balancers, [437](#)

 vSphere, [401, 407, 419](#)

Local Distance parameter (BGP timer policy), [342](#)

local endpoints, [242-243, 594](#)

local users

 access

assigning, [523-525](#)

modifying, [523-525](#)

 creating, [521-523](#)

Local-AS Number Config parameter (BGP peer connectivity profiles), [341](#)

Local-AS Number parameter (BGP peer connectivity profiles), [341](#)

locally governed ACI Multi-Site configurations, [557](#)

locked configuration items (function profiles), [445](#)

logical devices, [444, 446, 594](#). *See also device selection policies*

logical node and interface profiles, [295, 594](#)

login domains, [549-550](#)

login IDs, [522](#)

logit severity command, [498-499](#)

logs

- audit logs
 - definition of*, [127](#)
 - reviewing*, [127-128](#)
- blacklist EPG (endpoint group) with logging, [318-320](#)

longest prefix match (LPM), [175](#)

lookups, [90-92](#), [241-242](#)

Loop Detect Multiplication Factor setting (Global MCP Policy), [222](#)

Loop Protection Action setting (Global MCP Policy), [222](#)

loopback interfaces, [60](#)

LPM (longest prefix match), [175](#)

M

M3 APIC (Application Policy Infrastructure Controller) specifications, [33](#)

MAC address tables, [241](#)

MAC hashes, routes based on, [402](#)

MACsec, [173](#)

Maintenance state (fabric node discovery), [52](#)

Major faults, [112](#)

Manage VMkernel Adapters page (Add and Manage Hosts wizard), [413](#)

managed devices, deploying service graphs for, [453-460](#)

managed mode, [428, 430–432](#)

managed objects (MOs), [109, 594](#)

management

- in-band, [462](#)
 - access policies for APIC in-band interfaces*, [468–469](#)
 - APIC connectivity preferences*, [478–479](#)
 - bridge domains*, [469](#)
 - compared to out-of-band (OOB) management*, [48](#)
 - configuration steps for*, [467–468](#)
 - connectivity*, [465–467](#)
 - deployment alongside out-of-band (OOB) management*, [467](#)
 - in-band network, extending out of fabric*, [474–476](#)
 - IP addressing*, [470–474](#)
 - whitelisting desired connectivity to/from*, [476–477](#)
- management access modification, [103–105](#)
- MIBs (Management Information Bases), [501–502, 594](#)
- MIM (Management Information Model), [105–107](#)
- multitenancy, [13](#)
- out-of-band (OOB), [462](#)
 - compared to in-band management*, [48](#)
 - connectivity*, [464–465](#)
 - contracts*, [479–480](#)
 - deployment alongside in-band management*, [467](#)
- service graph management models
 - definition of*, [597](#)
 - network policy mode*, [428–430, 595](#)

overview of, 428
service manager mode, 428, 430–432–434, 597
service policy mode, 428, 430–432, 597
templates, 597

of traditional networks, 4–7

Management and Analytics System (MAS), 432

Management EPG parameter

LDAP providers, 542
RADIUS providers, 541
TACACS+ providers, 533

managers, SNMP (Simple Network Management Protocol), 500

mandatory configuration items (function profiles), 445

many-to-many relationships, 153

mapping ports, 191–194, 267–269

marking traffic, 218

Maximum AS Limit setting (BGP timer policy), 338

Maximum ECMP setting (OSPF timer policy), 329

Maximum Path Limit setting (EIGRP Context per Address Family), 325

maximum transmission units (MTUs), 25, 31

MCP (MisCabling Protocol), 388

configuration, 221–222
definition of, 594
interface policies, 172

MEC (Multichassis EtherChannel) technology, 6

Merge import type, 75

mergers, multitenancy and, 13

messages, system. See [system messages](#)

Metric Style setting (EIGRP Context per Address Family), 325

mgmt security domain, 517

mgmt tenants, 135

MIBs (Management Information Bases), 501-502

- definition of, 594
- scope of, 502, 592
- VRF-specific, 600

microsegmentation, 146

Migrate VM Networking page (Add and Manage Hosts wizard), 414

migration, VLAN, 385-386

MIM (Management Information Model), 105-107, 594

Minor faults, 112

MisCabling Protocol (MCP), 221-222, 388, 594

modes

- Pearson IT Certification test prep software, 568-569
- service graph deployment
 - network policy mode, 428-430, 595*
 - service manager mode, 428, 430-432-434, 597*
 - service policy mode, 428, 430-432, 597*

monCommonPol class, 118

monEPGPol class, 118

monFabricPol class, 118

monInfraPol class, 118

monitoring

health. See [health monitoring](#)

message forwarding to syslog servers, [485–492](#)

ACI severity levels, [485](#)

contracts for, [487–491](#)

NX-OS severity levels, [485](#)

steps for, [487](#)

syslog monitoring destination groups, [492–493](#)

syslog sources, [494–498](#)

verification of, [498–500](#)

service graphs, [447](#)

SNMP (Simple Network Management Protocol)

ACI support for, [501–502](#)

client group policies, [504–506](#)

configuration caveats, [502](#)

contexts, [506](#)

contracts, [503](#)

informs, [501](#)

SNMP agents, [500](#)

SNMP managers, [500](#)

SNMP monitoring destination groups, [507–508](#)

SNMP sources for desired monitoring policies, [508](#)

steps for, [502–503](#)

traps, [501](#)

verification of, [509–511](#)

versions of, [500–501](#)

monitoring destination group, [594](#)

monitoring sources, [594](#)

monPolDn attribute, [116-117](#), [594](#)

MOQuery, [110](#), [128](#), [499-500](#), [510-511](#), [595](#)

MOs (managed objects), [109](#), [594](#)

MP-BGP (Multiprotocol BGP), [23](#), [305-306](#)

MP-BGP EVPN (Multiprotocol Border Gateway Protocol Ethernet Virtual Private Network), [12](#)

MSO (Multi-Site Orchestrator), [15](#), [27](#), [555](#), [557](#)

MST (Multiple Spanning Tree) instance mappings, [387-388](#)

MTUs (maximum transmission units), [25](#), [31](#)

Multi Destination Flooding field (bridge domain settings), [370](#), [595](#)

Multicast PIM-Bidir support, [32](#)

Multichassis EtherChannel (MEC) technology, [6](#)

Multiple Spanning Tree (MST) instance mappings, [387-388](#)

Multiprotocol BGP (MP-BGP), [23](#)

Multiprotocol Border Gateway Protocol Ethernet Virtual Private Network (MP-BGP EVPN), [12](#)

Multi-Site. *See* [ACI Multi-Site](#)

Multi-Site Orchestrator (MSO), [15](#), [27](#), [555](#), [557](#)

multitenancy, [11-14](#), [549-550](#), [595](#). *See also* [tenants](#)

multitier application deployment

- application profiles, [264-266](#)
- BD (bridge domain) configuration, [264-266](#)
- DHCP (Dynamic Host Configuration Protocol) relay, [270](#)
- domain assignment, [267](#)

EPG (endpoint group) configuration, [264–266](#)
EPG (endpoint group) mapping to ports, [267–269](#), [270](#)
overview of, [263](#)
policy deployment, [270](#)
verification of EPG-to-port assignments, [269–270](#)

N

names, distinguished, [109](#), [591](#)
namespace normalization, [28](#)
navigation, APIC CLI (command-line interface), [101](#)
ND (Neighbor Discovery), [241](#)
nesting tenants, [134](#)
NetFlow, [171](#), [174](#)
netstat command, [86–87](#)
Network Failure Detection setting, [402](#)
network management touchpoints, [9–10](#)
network migrations into ACI
 Any EPG (vzAny), [364–365](#), [589](#)
 contract enforcement at VRF instance level, [367](#)
 endpoint learning considerations, [371–372](#)
 flooding requirements, [368–370](#)
 ARP Flooding, [369](#)
 Forwarding setting, [368](#)
 L2 Unknown Unicast, [368](#)
 L3 Unknown Multicast Flooding, [369](#)
 Multi Destination Flooding, [370](#)

full-mesh network-centric contracts, 362–364

GARP-based detection, 370–371

Legacy mode, 371

network-centric deployments, 361–362

overview of, 361

preferred group members, 365–367

preparation for, 372

security enforcement in, 362

network policy mode, 428–430, 595

Network Time Protocol. *See NTP (Network Time Protocol)*

network-centric deployments, 361–362

networks. *See also VLANs (virtual LANs); vSphere*

software-defined, 4

traditional

agility of, 8

management of, 4–5

scalability and growth of, 5–7

security of, 8–9

three-tier design of, 5–7

visibility of, 9

New Distributed Port Group wizard, 400

Next-hop Self parameter (BGP peer connectivity profiles), 340

Nexus 1000v distributed virtual switch, 9

Nexus 9332C switches, 38

Nexus 9336C-FX2 switches, 40, 215

Nexus 9336PQ switches, 37

Nexus 9364C switches, 38

Nexus 9732C-EX switches, 38

Nexus 9736C-FX switches, 38

Nexus 9736PQ switches, 37

Nexus 93180YC-EX switches, 40, 215

Nexus 93180YC-FX switches, 40, 45

Nexus 93240YC-FX2 switches, 40

Nexus 93360YC-FX2 switches, 40

NIC loads, routes based on, 402

no password pwd-strength-check command, 522-523

node ID, 11, 595

node management, 472-473

node profiles, 294, 295

Node Registration wizard, 57

node-level BGP (Border Gateway Protocol) customizations, 337-339

non-ACI switches, Layer 2 extension to

 ACI interaction with STP (Spanning Tree Protocol), 386-388

link types, 388

MCP (MisCabling Protocol), 388

MST (Multiple Spanning Tree) instance mappings, 387-388

TCNs (topology change notifications), 386-387

 Layer 2 connectivity to non-ACI switches

bridge domain extensions, 374-375

EPG (endpoint group) extensions, 372-373, 375-380

L2Outs, [380–385](#)

migration of overlapping VLANs into ACI, [385–386](#)

overview of, [372](#)

network migrations into ACI

- Any EPG (vzAny)*, [364–365, 589](#)
- contract enforcement at VRF instance level*, [367](#)
- endpoint learning considerations*, [371–372](#)
- flooding requirements*, [368–370](#)
- full-mesh network-centric contracts*, [362–364](#)
- GARP-based detection*, [370–371](#)
- Legacy mode*, [371](#)
- network-centric deployments*, [361–362](#)
- overview of*, [361](#)
- preferred group members*, [365–367](#)
- preparation for*, [372](#)
- security enforcement in*, [362](#)

overview of, [358](#)

north-south traffic, [7](#)

Notify Switches setting, [403](#)

NSX-T VDS, [395](#)

NTP (Network Time Protocol), [84–89, 106](#)

ntpstat command, [87](#)

N-VDS, [395](#)

nw-svc-admin role, [520](#)

nw-svc-params role, [520](#)

NX-OS, system message severity levels, [485](#)

O

object model, 96

correlation of menus to, [107-108](#)
exploring with Visore, [108-110](#)
faults in, [116-118](#)
importance of, 110
overview of, [105-107](#)
topRoot object, [106](#)

On Demand immediacy, 407

on-demand backups, 76-79

one-arm load balancers, 437

one-to-many relationships, 153

online access, Pearson IT Certification test prep software, 567

Operational faults, 113

operations, ACI Anywhere. See [ACI Anywhere](#)

ops role, 520

OSPF (Open Shortest Path First)

configuration for BGP L3Out, [344](#)

L3Out for OSPF peering

BFD (Bidirectional Forwarding Detection) implementation, 328-329

L3Out Creation Wizard, 325-327

OSPF timer policy, 329

OSPFv3 support, 344

route advertisement, 328

VRF-level customizations, 329

Remote Leaf deployments, 32

OTV (Overlay Transport Virtualization), 560

out-of-band (OOB) management, 462

- ACI fabric initialization and
 - automatic upgrades of new switches, 74–75*
 - default contracts, 64–66*
 - fabric upgrades, 66–71*
 - schedulers, 73, 597*
 - static out-of-band addresses, assignment of, 63–64*
- APICs (Application Policy Infrastructure Controllers), 47–48
 - connectivity, 464–465
 - contracts, 479–480
 - deployment alongside in-band management, 467
 - in-band management compared to, 48

outside EPGs (endpoint groups), 151–153

overlapping VLANs, migration into ACI, 385–386

overlay, 135

overlay multicast TEP, 555, 595

Overlay Transport Virtualization (OTV), 560

overlay unicast TEP, 555, 595

overrides

 - leaf interface, 232, 594
 - port channel member, 232–235, 596

P

packages, device. See **device packages, importing**

packet forwarding scenarios, 251

- both endpoints attach to same leaf, 251–254
- flooding to unknown destination, 261–263
- known destination behind another leaf, 254–258
 - learning and forwarding for vPCs, 256–258*
 - verification of traffic path between known endpoints, 254–256*
- spine proxy to unknown destination, 258–261

partnerships, multitenancy and, 13

Passive Participation option (OSPF), 329

Password parameter (LDAP providers), 542

Password Strength parameter (ACI fabric initialization), 49

Password Strength Policy, 522–523

Password/Confirm Password parameter (BGP peer connectivity profiles), 340

passwords

- BIOS, 52
- strength of, 522–523

PBR (policy-based redirect), 141, 427

PC/VPC override policy groups, 171

Pearson IT Certification test prep software, 567–568

- modes, 568–569
- offline access, 568
- online access, 567
- overview of, 567
- Premium Edition, 569–570
- updating, 569

peer connectivity profiles (BGP), 339–341

per-bridge domain settings, 560, 561

per-neighbor BGP (Border Gateway Protocol) customizations, 339–341

pervasive gateways, 252–254, 595

pervasive routes, 258–260, 595

Per-VLAN Spanning Tree (PVST+), 387–388

PFC (priority-based flow control), 172

physical domains, 161, 595

physical tunnel endpoint (PTEP), 60, 595

PI VLANs (platform-independent VLANs), 246, 253–254, 595

Ping Check setting (AAA policy), 548

ping command, 364, 474

planning

- ACI fabric initialization, 42, 44–45, 47–48, 51
 - APIC connectivity, 46–47*
 - APIC OOB configuration requirements, 47–48*
 - basic configuration parameters, 48–49*
 - cabling requirements, 45*
 - fabric discovery stages, 51–52*
 - out-of-band versus in-band management, 48*
 - switch discovery process, 49–51*
 - switch discovery states, 51–52*
- VMM (Virtual Machine Manager) integrations, 403–405

platform-independent VLANs (PI VLANs), 246, 253–254, 595

platforms, cross-platform integrations, 15

Pod 1 TEP Pool parameter (ACI fabric initialization),
49

pod ID parameter (ACI fabric initialization), **48**

pod policy, **83**

pod policy groups, **83-86, 595**

pod profiles, **83-84, 596**

pod selectors, **83, 596**

PoE (Power over Ethernet), **172, 175**

policies. *See also* **access policies; tenant policies**

AAA authentication, [547-550](#)

date/time, [84-89](#)

definition of, [110](#)

device selection, [446](#)

fabric, [106, 592](#)

fault management, [120-121](#)

health monitoring, [118-120](#)

keychain, [324](#)

LACP (Link Aggregation Control Protocol), [419-421](#)

password strength, [522-523](#)

pod, [83](#)

Policy Universe, [105, 106, 109, 596](#)

primary and disaster recovery data center deployments,
[561-562](#)

reuse of, [16](#)

route control, [351-352](#)

SNMP (Simple Network Management Protocol), [504-506](#)

timer

BGP (Border Gateway Protocol), 337–339, 342

OSPF (Open Shortest Path First), 329

VMware vSphere, 400–403

policing, 218

Policy Universe, 105, 106, 109, 596

policy-based redirect (PBR), 141, 427

pools

TEP (tunnel endpoint), 49, 50, 57, 59, 599

VLAN (virtual LAN), 159–160, 599

creating, 159–160

designs for, 161–163

overlap between, 164–165

static versus dynamic VLAN allocation, 159, 598

VLAN ranges in, 160

port bindings, 400, 596

port blocks, 198–199

port channel member overrides, 232–235, 596

port channels

configuration, 196–201

interface policies and interface policy groups, 170, 171

member overrides, 232–235, 596

members, 172

vPCs (virtual port channels), 6

configuration, 204–207

domains, 201–204

learning and forwarding for, 256–258

VIP addresses, 245

port encapsulation VLANs, 246, 596

port groups

definition of, 395–397, 596

distributed, 397

assigning VMs (virtual machines) to, 417–418

pushing EPGs (endpoint groups) to vCenter as, 415–416

Port Local Scope, 385–386

Port parameter

LDAP providers, 542

TACACS+ providers, 532

port security interface policies, 173

PortFast, 387

ports

ACI switch port configurations

AAEP EPGs (endpoint groups), 207–210

implications of, 210

individual port configuration, 188–196

overview of, 186–188

port channel configuration, 196–201

vPC (virtual port channel) configuration, 204–207

vPC (virtual port channel) domain configuration, 201–204

APIC (Application Policy Infrastructure Controller), 46–47, 589

bindings, 400, 596

blocks, 198–199

dynamic breakout ports, 215–217, 591

encapsulation, 246
fabric, 23, 592
mappings, 191-194, 267-269
port groups, 395-397
 definition of, 596
 distributed, 397, 415-418
Port Local Scope, 385-386
usage types, 195
VMware vSphere, 400

Power over Ethernet (PoE), 172, 175

power supplies, 46

Practice Exam mode, Pearson IT Certification test prep software, 568-569

preferred group members, 365-367, 596

Prefix Suppression setting (OSPF timer policy), 329

Premium Edition, Pearson IT Certification test prep software, 569-570

Pre-Provision immediacy, 405-406

primary data center deployments, 558-562

centralized orchestration and management capabilities, 559
cross-data center ingress routing optimization, 561-562
overview of, 558-559
per-bridge domain broadcast and stretch settings, 560

priority flow control interface policies, 172

priority levels, 218

priority-based flow control (PFC), 172

private networks. *See* **VRF (virtual routing and forwarding) instances**

privileges

- definition of, [596](#)
- expanding, [523-525](#)
- for predefined roles, [519-521](#)

Production/EPG-Admin/ value, [540](#)

profiles, [176-179](#)

- AAEPs (attachable access entity profiles), [165-169](#), [382](#)
 - configuration*, [167-169](#), [190-191](#)
 - definition of*, [589](#)
 - EPGs (endpoint groups)*, [207-210](#)
 - in-band management*, [468](#)
 - in L3Out domains*, [302](#)
 - overview of*, [165-166](#)
- application, [527](#)
 - advantages of*, [138-139](#)
 - configuration*, [142-145](#)
 - definition of*, [138](#), [589](#)
 - multitier application deployment*, [264-266](#)
 - topology*, [138-139](#)
- custom function, [444-445](#)
- DNS (Domain Name System) server, [86-92](#)
- external management network instance, [491](#)
- FEX (fabric extenders), [213-214](#)
- forwarding scale, [175](#)
- function, [592](#)

custom, [444–445](#)
examples of, [430–433](#), [442](#)
interface, [179–182](#)
logical node and interface, [295](#), [594](#)
pod, [83–84](#), [596](#)
route, [344–345](#), [597](#)
switch, [179–182](#), [598](#)
TACACS+, [537–538](#)
VMM (Virtual Machine Manager) domain, [408–410](#)

programmability, ACI (Application Centric Infrastructure), [11](#)

providers, [149–150](#), [596](#)

proxy, hardware, [247–248](#)

proxy TEP addresses, [61](#)

PTEP (physical tunnel endpoint), [60](#), [595](#)

public clouds, extending ACI to, [564–565](#)

- with ACI Multi-Site, [564](#)
- with remote leaf switches, [564–565](#)
- with vPod, [564](#)

PVST+ (Per-VLAN Spanning Tree), [387–388](#)

Python SDK (software development kit), [103](#)

Q-R

QoS (quality of service), [217–219](#)

queueing, [218](#)

RADIUS, ACI configuration for, [540–541](#)

Raised state (faults), [114](#)

Raised-Clearing state (faults), 115

ranges, VLAN, 160

Rapid PVST+ (Rapid Per-VLAN Spanning Tree), 387-388

RARP (Reverse ARP), 403

RAT (Resource Allocation Timeout), 175

RBAC (role-based access control), 133, 514

- access, 523-525-528
- common pitfalls in, 531
- custom rules, 528-531
- local users
 - assigning access to, 523-525*
 - creating, 521-523*
 - modifying access for, 523-525*
- multitenancy and, 13
- overview of, 516-517
- privileges
 - expanding, 523-525*
 - for predefined roles, 519-521*
- roles
 - modifying, 523-525-528*
 - predefined, 519-521*
- rules, 596
- security domains, 517-518
 - assigning tenants to, 517-518*
 - creating, 517*
 - definition of, 517*

predefined, 517

read queries, 501

read-all role, 520

recovery, Error Disabled Recovery Policy, 231–232

relay, DHCP (Dynamic Host Configuration Protocol), 219–221, 271

reload command, 100

remote endpoint learning, 244–245

remote endpoints, 242–243, 596

remote leaf switches, 564–565

Remote Leaf topology, 30–32

remote locations, extending ACI to, 564–565

- with ACI Multi-Site, 564
- with remote leaf switches, 564–565
- with vPod, 564

Remote User Login Policy setting (AAA policy), 548

remoteleaf role, 57

Remove All Private AS parameter (BGP peer connectivity profiles), 340

Remove Private AS parameter (BGP peer connectivity profiles), 340

Replace import type, 75

Replace Private AS with Local AS parameter (BGP peer connectivity profiles), 341

representational state transfer. See REST (representational state transfer) API

resolution immediacy, 405–407, 596

Resource Allocation Timeout (RAT), 175

REST (representational state transfer) API, 11, 98

restores

- configuration backups, importing, 80–82
- configuration exports, 75
- configuration imports, 75–76
- configuration rollbacks, 82–83
- configuration snapshots, 80
- on-demand backups, 76–79
- scheduled backups, 79–80

Retaining state (faults), 115

Retention Interval timer, 115

Retries parameter

- LDAP providers, 542
- RADIUS providers, 540
- TACACS+ providers, 532

Reverse ARP (RARP), 403

Reverse Filter Ports feature, 277–278, 476

RIB (Routing Information Base), 241, 242

RJ-45 connectors, 46

role-based access control. See RBAC (role-based access control)

roles

- definition of, 596
- modifying, 523–525–528
- predefined, 519–521

Rollback to This Configuration option, 82

rollbacks, configuration, 82–83

roots, L3Out, 294

route advertisement

for EIGRP (Enhanced Interior Gateway Routing Protocol)
L3Outs, 328

for OSPF (Open Shortest Path First) L3Outs, 328

route control

inbound route filtering, 352–353

overview of, 344–345

policies for, 351–352

route attributes to all peers, 346–349

route attributes to specific peer, 349–351

route profiles, 344–345, 597

Route Control Profile parameter (BGP peer connectivity profiles), 341

route leaking, 466

route peering, 438–439

route profiles, 597

route reflection, BGP (Border Gateway Protocol)

definition of, 597

implementation of, 304–305

infra MP-BGP route distribution, 305–306

need for, 303–304

routed mode, devices in, 435

Routing Information Base (RIB), 241, 242

rules, RBAC (role-based access control), 528–531, 596

running configuration, viewing, 102

S

satellite/small colo data centers, Remote Leaf deployments for, 30

Save & Exit Setup dialog box, 52

scalability

ACI (Application Centric Infrastructure), 10

APIC (Application Policy Infrastructure Controller) clusters, 33–36

traditional networks, 5–7

Schedule Controller Upgrade page, 67–69

Schedule Node Upgrade window, 70

scheduled backups, 79–80

schedulers, 73, 597

schemas, 557–558, 597

scope

of contracts, 150–151, 284–285, 590

of MIBs (Management Information Bases), 502, 592

Port Local, 385–386

SVI Encap, 298–299

SCP (Secure Copy Protocol), 67

scripts, setup-clean-config.sh, 100

SDN (software-defined networking), 4

secondary IP addresses, 325–326, 597

secondary keyword, 147

second-generation leaf switches, 39–40

second-generation spine switches, 37–38

Secure Copy Protocol (SCP), 67

security domains, 517-518

- assigning tenants to, 517-518
- creating, 517
- definition of, 517, 597
- mapping domains to, 526-528
- predefined, 517

seed leaf initialization, 51

Select New Hosts page (Add and Manage Hosts wizard), 412

selectors, 83, 176-179

Self Nexthop, 324

Send Community parameter (BGP peer connectivity profiles), 340

Send Extended Community parameter (BGP peer connectivity profiles), 340

serial ports (RJ-45 connector), 46

Server Monitoring parameter

- LDAP providers, 542
- RADIUS providers, 541
- TACACS+ providers, 533

servers

DNS (Domain Name System), 90-92

ESXi

- adding to VDS (vSphere distributed switches), 411-414*
- connecting in UCS domains, 407*
- connecting to fabric, 407*
- definition of, 395*
- standard switch architecture, 395*

VMkernel interface, [397–399](#)

vSphere distributed switches (VDS), [397](#)

external AAA server integration, [532](#)

- AAA authentication policy settings*, [547–550](#)
- ACI configuration for LDAP*, [541–547](#)
- ACI configuration for RADIUS*, [540–541](#)
- ACI configuration for TACACS+*, [532–536](#)
- Cisco AV pair formatting*, [538–540](#)
- ISE (Identity Service Engine) configuration*, [536–538](#)

syslog, forwarding system messages to

- contracts for*, [487–491](#)
- steps for*, [487](#)
- syslog monitoring destination groups*, [492–493](#)
- syslog sources*, [492–493](#)
- verification of*, [498–500](#)

service chains, [440, 450, 452, 597](#)

service graphs, [424](#)

- bridge domain settings for, [439–440](#)
- as concatenation of functions, [427–428](#)
- contracts for, [427–428](#)
- definition of, [597](#)
- deployment
 - for devices in GoThrough Mode*, [436, 437](#)
 - for devices in GoTo Mode*, [435, 436–437](#)
 - for one-arm load balancers*, [437](#)
- dynamic endpoint attach, [439](#)
- implementation examples

service graphs for managed devices, [453–460](#)

unmanaged firewall pair deployment, [447–452](#)

implementation workflow

custom function profiles, [444–445](#)

device package imports, [430, 441–442](#)

device selection policy configuration, [446](#)

L4-L7 device identification, [443–444](#)

overview of, [441](#)

service graph monitoring, [447](#)

service graph parameters, [447](#)

service graph template configuration, [445–446](#)

service graph template instantiation, [446–447](#)

L4-L7 services integration, [435–436](#)

management models

network policy mode, [428–430, 595](#)

overview of, [428](#)

service manager mode, [428, 430–434, 597](#)

service policy mode, [428, 430–432, 597](#)

monitoring, [447](#)

overview of, [426–427](#)

parameters, [447](#)

with policy-based redirect (PBR), [427](#)

rendering, [440–441](#)

route peering, [438–439](#)

templates

configuration, [445–446](#)

definition of, [597](#)

instantiation of, [446–447](#)

when to use, [434–435](#)

without policy-based redirect (PBR), [427](#)

service leaf switches, [24, 597](#)

service manager mode, [428, 430–432, 597](#)

service policy mode, [428, 430–432, 597](#)

service VM orchestration, [428](#)

service-level agreement (SLA) tracking, [330–334](#)

setup-clean-config.sh, [100](#)

severity levels

- ACI, [485](#)
- faults, [111–112, 121–124](#)
- NX-OS, [485](#)

shadow EPGs (endpoint groups), [428–429, 597](#)

sharding, database, [34–35, 597–598](#)

shared configuration items (function profiles), [445](#)

shared service, [293](#)

shell:domains value assignments, [539–540](#)

shells

- bash, [102](#)
- Broadcom, [103](#)
- VSH (Virtual Shell), [103](#)
- vsh_lc, [103](#)

show bgp ipv4 unicast vrf all command, [304](#)

show bgp process detail vrf all command, [304](#)

show bgp sessions vrf overlay-1 command, [306](#)

show bgp vpng4 unicast vrf overlay-1 command, [304](#)

show copp policy command, 226-229
show endpoint ip command, 252, 258
show fex command, 214
show interface ethernet 1/45-46 status command, 194
show interface tunnel 1-20 command, 62
show ip arp vrf command, 314
show ip bgp command, 348
show ip dhcp relay command, 271
show ip eigrp neighbors command, 313
show ip int brief command, 60
show ip int brief vrf command, 61, 270
show ip route command, 136-137, 258
show ip route vrf command, 136-137, 270, 313
show isis adjacency detail vrf overlay-1 command, 60
show isis dteps vrf overlay-1 command, 61, 259
show lacp interface command, 233-235
show ntp peers command, 87-88
show ntp peer-status command, 87-88
show ntp statistics peer ipaddr command, 88
show port-channel summary command, 199-200, 206-207, 214, 233
show run command, 536, 541
show run tenant DCACI command, 147
show running-config all command, 195, 207
show running-config command, 102
show running-config dns command, 102

show running-config leaf-interface-profile command, 182, 215

show running-config vlan-domain DCACI-Domain command, 169

show snmp command, 509-510

show snmp summary command, 510

show system internal epm endpoint ip command, 256

show system internal epm vpc command, 257

show track command, 333

show vlan extended command, 246-247, 270, 386

show vpc command, 204, 206

show vrf command, 136-137

show vrf Production:MP detail extended command, 247

show zoning-rule command, 284

silent hosts, 245-247, 248-249

Simple Network Management Protocol. See [SNMP \(Simple Network Management Protocol\)](#)

site IDs, 555, 598

sites, 555, 598

sizing APIC (Application Policy Infrastructure Controller) clusters, 33-36

SLA (service-level agreement) tracking, 330-334

slow drain interface policies, 173

snapshots, configuration, 80

SNAT (source NAT), 436

SNMP (Simple Network Management Protocol)

 ACI support for, 501-502

agents, 500
client group policies, 504–506
configuration caveats, 502
contexts, 506
contracts, 503
informs, 501
managers, 500
monitoring destination groups, 507–508
notifications, 598
sources for desired monitoring policies, 508
steps for, 502–503
traps, 501, 598
verification of, 509–511
versions of, 500–501

snooping, IGMP (Internet Group Management Protocol), 368

Soaking Interval timer, 115

Soaking state (faults), 114

Soaking-Clearing state (faults), 114

software, Pearson IT Certification test prep software, 567–568

modes, 568–569
offline access, 568
online access, 567
overview of, 567
Premium Edition, 569–570
updating, 569

software development, multitenancy and, 13

software-defined networking (SDN), 4

source NAT (SNAT), 436

sources, SNMP (Simple Network Management Protocol), 508

SPAN (Switched Port Analyzer), 219

spanning tree interface policies, 172

spanning-tree link type point-to-point command, 388

spanning-tree link type shared command, 388

spanning-tree port type edge command, 387

spanning-tree port type edge trunk command, 387

spine hardware, 23, 36

spine proxy, 61, 247-248

spine switches

- definition of, 22, 598
- first-generation, 37
- second-generation, 37-38
- spine initialization, 51

spine-and-leaf architecture, 9-10

split horizon, 324

squelching, 127, 598

SSL Certificate Validation Level parameter (LDAP providers), 542

Stale Interval (BGP timer policy), 338

standard ACI topology, 22-24

standby controller parameter (ACI fabric initialization), 48

stateful-services integration, 563-564

stateless networking, 11, 182-183

states

faults, 114-115

switch discovery, 51-52

static bindings, mapping EPGs (endpoint groups) to ports with, 267-269

static IP addressing, 470-472

Static Node Management Addresses folder, 64

static out-of-band addresses, 63-64

static port bindings, 400

static port channeling, 204-205

static routes, adding on L3Outs, 329-330-334

static VLAN allocation, 159, 598

storm control, 172, 223-224

STP (Spanning Tree Protocol), ACI interaction with, 386-388

link types, 388

MCP (MisCabling Protocol), 388

MST (Multiple Spanning Tree) instance mappings, 387-388

TCNs (topology change notifications), 386-387

stretch settings, 560

stretched fabric topology, 24-25, 598

stretched objects, 557, 598

stub network and transit routing, 291-292

Study mode, Pearson IT Certification test prep software, 568-569

subjects

for bidirectional application, 275-276
definition of, 148-149, 598
for unidirectional application, 280-281
verification of, 278

subnets, 469-470

advertising, 314-315
limiting endpoint learning to, 249-250
subnet boundaries, designing around, 139-141

Suspend Individual Port setting, 197, 201

SVIs (switch virtual interfaces), 147

Auto State, 299-300
Encap Scope, 298-299
floating, 296, 592

switch CLI, 102-103

switch policies, 174-176

switch policy groups, 174-176

switch port configurations

AAEP EPGs (endpoint groups), 207-210
implications of, 210
individual port configuration, 188-196

AAEPs (attachable access entity profiles), 190-191, 589

CDP interface policy, 190
common control settings, 196-198
leaf access port policy groups, 191
link level interface policy, 189
LLDP interface policy, 189

port blocks, [198-199](#)
port mappings, [191-194](#)
port usage types, [195](#)
verification of, [194](#)
overview of, [186-188](#)
port channel configuration, [196-201](#)
vPC (virtual port channel) configuration, [204-207](#)
 with APIC CLI, [207](#)
 static port channeling, [204-205](#)
 verification of, [206-207](#)
 vPC interface policy groups, [205-206](#)
vPC (virtual port channel) domains, [201-204](#)

switch profiles, [179-182, 598](#)

switch selectors, [179, 598](#)

switch virtual interfaces. *See also* **SVIs (switch virtual interfaces)**

Switched Port Analyzer (SPAN), [219](#)

switches. *See also* **non-ACI switches, Layer 2 extension to**

 ACI fabric initialization and
 automatic upgrades of new switches, [74-75](#)
 connectivity following switch initialization, [59-62](#)
 default contracts, [64-66](#)
 discovery and activation, [55-58](#)
 discovery process, [49-51](#)
 discovery states, [51-52](#)
 static out-of-band addresses, assignment of, [63-64](#)

verification of, 59-62

ACI switch port configurations

AAEP EPGs (endpoint groups), 207-210

implications of, 210

individual port configuration, 188-196

overview of, 186-188

port channel configuration, 196-201

vPC (virtual port channel) configuration, 204-207

vPC (virtual port channel) domains, 201-204

CLI (command-line interface), [100-102](#)

leaf, [9-11](#)

border, 24, 590

cabling requirements, 45

compute, 24, 590

definition of, 22, 594

first-generation, 38-39

initialization of, 51

IP storage, 24, 593

leaf access port policy groups, 191

overview of, 23

pervasive gateways, 252-254, 595

pervasive routes, 258-260, 595

profiles, 179-182

purchasing decisions, 38

remote, 564-565

second-generation, 39-40

service, 24, 597

transit, 25, 599

Nexus 1000v distributed virtual switch, 9

packet forwarding scenarios, 251

both endpoints attach to same leaf, 251–254

flooding to unknown destination, 261–263

known destination behind another leaf, 254–258

spine proxy to unknown destination, 258–261

spine

definition of, 22, 598

first-generation, 37

overview of, 23

second-generation, 37–38

spine initialization, 51

SVIs (switch virtual interfaces), 147

Auto State, 299–300

Encap Scope, 298–299

floating, 296

VDS (vSphere distributed switch), VMM integration with, 392, 405

advantages of, 403

enhanced LACP policy support, 419–421

EPGs, pushing to vCenter as distributed port groups, 415–416

ESXi connectivity, 407

ESXi hosts, adding to VDS, 411–414

immediacy settings, 405–407

NSX-T VDS, 395

N-VDS, [395](#)

planning, [403–405](#)

prerequisites for, [403, 407](#)

VDS deployment, [405](#)

VM assignment to distributed port groups, [417–418](#)

VMM domain association settings, [418](#)

VMM domain profiles, [408–410](#)

vSwitches (vSphere standard switches), [395, 600](#)

Switch-Facing-Interface policy, [375](#)

Symmetric Hashing setting, [197](#)

synchronization, NTP (Network Time Protocol), [84–89, 106](#)

syntax, system message, [485–492](#)

syslog monitoring destination groups, [492–493](#)

syslog servers, forwarding system messages to

contracts for, [487–491](#)

steps for, [487](#)

syslog monitoring destination groups, [492–493](#)

syslog sources, [494–498](#)

verification of, [498–500](#)

System Health panel, [124](#)

system messages

ACI severity levels, [487](#)

definition of, [598](#)

forwarding to syslog servers

contracts for, [487–491](#)

steps for, [487](#)

syslog monitoring destination groups, [492–493](#)
syslog sources, [494–498](#)
 verification of, [498–500](#)
NX-OS severity levels, [485](#)
syntax, [485–492](#)

T

tables

DHT (distributed hash table), [92](#)
lookup, [241–242](#)

TACACS+, ACI configuration for, [532–536](#)

TCNs (topology change notifications), [386–387](#)

TCP (Transmission Control Protocol), [279–280](#)

teaming, VMware vSphere, [400–403](#)

Telco 5G distributed data centers, Remote Leaf deployments for, [30](#)

template conformity, [557, 599](#)

templates

ACI Multi-Site, [557–558](#)
definition of, [598](#)
service graphs
 configuration, [445–446](#)
 definition of, [597](#)
 instantiation of, [446–447](#)

tenant DCACI command, [147](#)

tenant policies. *See also access policies; endpoint learning*

multitier application deployment, [263](#)
application profiles, [264-266](#)
BD (bridge domain) configuration, [264-266](#)
DHCP (Dynamic Host Configuration Protocol) relay, [271](#)
domain assignment, [267](#)
EPG (endpoint group) configuration, [264-266](#)
EPG (endpoint group) mapping to ports, [267-269](#), [270](#)
overview of, [263](#)
policy deployment, [270](#)
verification of EPG-to-port assignments, [269-270](#)

packet forwarding scenarios, [251](#)
both endpoints attach to same leaf, [251-254](#)
flooding to unknown destination, [261-263](#)
known destination behind another leaf, [254-258](#)
spine proxy to unknown destination, [258-261](#)

tenant-admin role, [520](#)

tenant-a-l3domain, [162](#), [164](#)

tenant-a-pdomain, [162](#), [164](#)

tenant-b-l3domain, [162](#), [164](#)

tenant-b-pdomain, [162](#), [164](#)

tenant-c-l3domain, [162](#), [164](#)

tenant-c-pdomain, [162](#), [164](#)

tenant-ext-admin role, [520](#)

tenants. *See also contracts; EPGs (endpoint groups); L3Outs; tenant policies; VRF (virtual routing and forwarding) instances*

access policies and, [184](#)

APIC CLI configuration, [147](#)
application profiles, [527](#)
 advantages of, 138-139
 configuration, 142-145
 definition of, 138
 topology, 138-139
assigning to security domains, [517-518](#)
BDs (bridge domains)
 advertisement of subnets assigned to, 314-315
 configuration, 142-145
 definition of, 137, 590
 DHCP (Dynamic Host Configuration Protocol), 271
 disabling endpoint learning on, 250-251
 extensions, 374-375
 external, 161, 380-385, 591
 in-band management, 469
 L3Out, 296-298, 594
 multitier application deployment, 264-266
 practical application of, 141-142
 service graph settings, 439-440
connectivity outside the fabric, [151-153](#)
 external EPGs (endpoint groups), 151-153
 Layer 3 Outside (L3Out), 153
creating, [133-134](#)
definition of, [133, 599](#)
hierarchy, [153-154](#)
multitenancy, [11-14, 549-550, 595](#)

nesting, [134](#)
predefined, [134-135](#)
use cases for, [133](#)

tenant-security privilege, [519](#)

TEPs (tunnel endpoints)

overlay multicast, [555, 595](#)
overlay unicast, [555, 595](#)
PTEP (physical tunnel endpoint), [60, 595](#)
TEP pools, [49, 50, 57, 59, 599](#)
verifying addresses of, [60-62](#)
VTEP, [31-32, 245, 256-258](#)

Tetration, [272](#)

three-tier Clos topology, [22](#)

three-tier network design, [5-7](#)

tier-2-leaf role, [57](#)

time/date, NTP (Network Time Protocol) synchronization, [84-89, 106](#)

Timeout parameter

LDAP providers, [542](#)
RADIUS providers, [540](#)
TACACS+ providers, [532](#)

timer policy

BGP (Border Gateway Protocol), [337-339, 342](#)
OSPF (Open Shortest Path First), [329](#)

timers, lifecycle, [115](#)

timestamps, [485](#)

topologies, [18, 21](#)

ACI Multi-Pod
 active/active data center deployments, 562–564
 overview of, 25–26
 stateful-services integration, 563–564

ACI Multi-Site, [555–558](#)
 cross-site connectivity, 555–557
 extending ACI to remote locations and public clouds, 564
 locally governed configurations, 557
 MSO-governed configurations, 557
 overview of, 26–28
 primary and disaster recovery data center deployments, 558–562
 schemas, 557–558
 stateful-services integration, 563–564
 terminology for, 557

ACI Multi-Tier, [28–30](#)

ACI stretched fabric, [24–25, 598](#)

Clos, [21–22](#)

Remote Leaf, [30–32](#)

standard ACI, [22–24](#)

topology change notifications (TCNs), 386–387

topRoot object, 106

tracking, service-level agreement, 330–334

traditional networks

 agility of, 8

 management of, [4–5](#)

scalability and growth of, 5-7

security of, 8-9

three-tier design of, 5-7

visibility of, 9

transit leaf switches, 25, 599

Transmission Frequency setting (Global MCP Policy), 222

transparent mode, devices in, 436

traps, SNMP (Simple Network Management Protocol), 501, 598

Trunk port-binding mode, 268

tunnel endpoints. See TEPs (tunnel endpoints)

tunnel interfaces, 62

U

UCS (Unified Computing System) domains, 218, 407

underlay, 135

Undiscovered state (fabric node discovery), 52

unicast routing, 243-244, 371

Unified Computing System (UCS) domains, 218, 407

Unknown state (fabric node discovery), 52

unmanaged firewall pairs, 447-452

unmanaged mode, 428-430

Unsupported state (fabric node discovery), 52

updates

DCACI 300-620 exam, 586-587

Pearson IT Certification test prep software, 569

upgrades

ACI fabric, [66–71](#)

EPLD (electronic programmable logic device), [66](#)
switches, [74–75](#)

USB ports, 46

uSeg EPGs (endpoint groups), 146

User Certificate Attribute setting (User Identity), 522–523

user identity groups, 536

User Identity page (Create Local User wizard), 522– 523

User VRF L3Outs (VRF-lite), 292

users. *See also* tenants

local

assigning access to, 523–525

creating, 521–523

modifying access for, 523–525

user identity groups, [536](#)

UTC (Coordinated Universal Time), 89

V

vCenter

failure, [399](#)

pushing EPGs (endpoint groups) to, [415–416](#)

vCenter Domain Creation wizard, 408–410

VDS (vSphere distributed switch), VMM integration with, 392

advantages of, 403
architecture, 397
definition of, 600
enhanced LACP policy support, 419–421
EPGs, pushing to vCenter as distributed port groups, 415–416
ESXi hosts, adding to VDS, 411–414
ESXi servers
adding to VDS, 411–414
connecting in UCS domains, 407
connecting to fabric, 407
immediacy settings, 405–407
NSX-T VDS, 395
N-VDS, 395
planning, 403–405
prerequisites for, 403, 407
VDS deployment, 405
VM assignment to distributed port groups, 417–418
VMM domain association settings, 418
VMM domain profiles, 408–410

Verified Scalability Guide, 24, 26, 34

VGA video ports, 46

VIC 1455 ports, 46–47

VIP addresses, 245

virtual APIC (Application Policy Infrastructure Controller) specifications, 33

virtual LANs. See [VLANs \(virtual LANs\)](#)

virtual leaf (vLeaf), 564

Virtual Machine Manager integrations. *See VMM (Virtual Machine Manager) integration*

virtual machines. *See VMs (virtual machines)*

virtual network interface cards (vNICs), 395, 400, 406, 414, 417, 465, 599

Virtual Pod (vPod), 26

virtual port channels. *See vPCs (virtual port channels)*

virtual routing and forwarding. *See VRF (virtual routing and forwarding) instances*

Virtual Shell (VSH), 103

virtual spine (vSpine), 564

virtualleaf roles, 57

virtualspine roles, 57

Visore, 108-110, 599

VLAN (virtual LAN) pools, 159-160, 599

creating, 159-160

designs for, 161-163

hybrid approach, 162-163

single VLAN pool for each type of domain, 161

single VLAN pool per function, 162

in L3Out domains, 301-302

overlap between, 164-165

static versus dynamic VLAN allocation, 159, 598

VLAN ranges in, 160

VLANs (virtual LANs)

access encapsulation, 246

dynamic VLAN allocation, 591
infrastructure, 593
overlapping, 385-386
PI VLANs (platform-independent VLANs), 246, 253-254, 595
pools, 159-160, 599
creating, 159-160
designs for, 161-163
in L3Out domains, 301-302
overlap between, 164-165
static versus dynamic VLAN allocation, 159, 598
VLAN ranges in, 160
port encapsulation, 246, 596
types of, 245-247
VLAN IDs, 245-247, 253-254
vLeaf (virtual leaf), 564
vmk0 interface, 397-399
VMkernel, 395, 397-399, 405, 406, 413-414, 599
VMM (Virtual Machine Manager) integration, 161, 599
advantages of, 403
definition of, 392
domains, 599
ESXi servers
connecting in UCS domains, 407
connecting to fabric, 407
immediacy settings, 405-407
for multiple data centers, 563

planning, 403–405
prerequisites for, 403, 407
VDS deployment, 405
VMM (Virtual Machine Manager) integration, 161

vmm-admin role, 520
VMM-NONPROD, 163, 164
VMM-PROD, 162, 164
VMM-VOICE, 163, 164
vmnic, 395, 413, 599
vMotion, 399

VMs (virtual machines)

assigning to distributed port groups, 417–418
VMware ESXi, 27

VMware ESXi. See [ESXi](#)

VMware vSphere

definition of, 392
distributed port groups, 397
 assigning VMs (virtual machines) to, 417–418
 pushing EPGs (endpoint groups) to vCenter as, 415–416
load balancing, 401, 407, 419, 600
overview of, 394–395
port bindings, 400
port groups, 395–397
system traffic
 impact of vCenter failure on, 399
 overview of, 397–399

teaming and failover policies, [400–403](#)

VMM integration with vSphere VDS, [392](#)

- advantages of, [403](#)*
- architecture, [397](#)*
- definition of, [600](#)*
- enhanced LACP policy support, [419–421](#)*
- EPGs, pushing to vCenter as distributed port groups, [415–416](#)*
- ESXi hosts, adding to VDS, [411–414](#)*
- ESXi servers, [407, 411–414](#)*
- immediacy settings, [405–407](#)*
- NSX-T VDS, [395](#)*
- N-VDS, [395](#)*
- planning, [403–405](#)*
- prerequisites for, [403, 407](#)*
- VDS deployment, [405](#)*
- VM assignment to distributed port groups, [417–418](#)*
- VMM domain association settings, [418](#)*
- VMM domain profiles, [408–410](#)*

vSwitches (vSphere standard switches), [395, 494–498, 600](#)

vNICs (virtual network interface cards), [395, 400, 406, 414, 417, 465, 599](#)

VNIDs (VXLAN network identifiers), [10, 28, 244, 245–247](#)

vpc domain explicit 21 leaf 101 102 command, [203](#)

VPC Explicit Protection Group wizard, [202](#)

VPC interface policy groups, [170](#)

vPC peer dead interval, 203, 599

vPCs (virtual port channels), 6

configuration, 204-207

with APIC CLI, 207

static port channeling, 204-205

verification of, 206-207

vPC interface policy groups, 205-206

domains, 201-204

learning and forwarding for, 256-258

VIP addresses, 245

vPC peer dead interval, 203, 599

vPod, 26, 564

VRF (virtual routing and forwarding) instances, 135-137

BGP customizations, 342-343

creating, 135-137

data plane learning, disabling, 251

definition of, 135, 599

EIGRP customizations, 324-325

for in-band management, 465-466, 474

multitenancy and, 12-13

OSPF customizations, 328-329

for out-of-band (OOB) management, 465

preferred group members, 365-367

SNMP contexts for, 506

User VRF L3Outs (VRF-lite), 292

VRF-specific MIB, 600

vrf context command, [147](#)
vrf member command, [147](#)
VSH (Virtual Shell), [103](#)
vsh_lc, [103](#)
vSphere. *See* [VMware vSphere](#)
vSpine (virtual spine), [564](#)
vSwitches (vSphere standard switches), [395](#), [494-498](#), [600](#)
VTEP, [31-32](#), [245](#), [256-258](#)
VXLAN network identifiers (VNIDs), [10](#), [28](#), [165](#), [244](#), [245-247](#)

W

Warning faults, [112](#)
Weight for routes from this neighbor parameter (BGP peer connectivity profiles), [340](#)
whitelisting, [14-15](#), [148-151](#), [427](#)
contracts
 additional whitelisting examples, [282-283](#)
 Apply Both Directions feature, [277-278](#)
 assigning to EPGs, [278-279](#)
 definition of, [148-149](#)
 direction of, [149-150](#)
 filters, [148-149](#), [273-275](#), [280](#)
 overview of, [272](#)
 planning enforcement of, [272-273](#)
 Reverse Filter Ports feature, [277-278](#)

scope of, [150-151, 284-285](#)
Stateful feature, [284](#)
subjects, [148-149, 278](#)
subjects for bidirectional application, [275-276](#)
subjects for unidirectional application, [280-281](#)
TCP established session rule, [279-280](#)
verifying enforcement of, [283-284](#)
zero-trust networks and, [151](#)
definition of, [600](#)
for in-band management, [476-477](#)

wizards

Add and Manage Hosts, [411-414](#)
BFD Interface Profile Creation, [322-323](#)
Configure Interface, PC, and VPC, [211-212](#)
Create Application EPG, [265-266](#)
Create Application Profile, [144-146](#)
Create Bridge Domain, [142-144, 264-265](#)
Create Bridged Outside, [380-385](#)
Create Configuration Export Policy, [76-78, 80-81](#)
Create DHCP Relay Label, [271](#)
Create Filter, [488](#)
Create LDAP Group Map Rules, [543-547](#)
Create LDAP Provider, [543](#)
Create Leaf Interface Profile, [179-180](#)
Create Leaf Profile, [180-181](#)
Create Local User, [521-523](#)
Create Physical Domain, [163](#)

Create RBAC Rule, [529–531](#)
Create Remote Location, [77](#)
Create Syslog Source, [494–495](#)
Create Tenant, [133–134](#)
Create VLAN Pool, [159–160](#)
Create VPC Explicit Protection Group, [202–203](#)
Create VRF, [135–137](#)
External EPG Creation, [310–312](#)
L3Out Creation
AAEPs (attachable access entity profiles), [302](#)
configuration for BGP peering, [334–337](#)
configuration for EIGRP peering, [307–309](#)
configuration for OSPF peering, [325–327](#)
New Distributed Port Group, [400](#)
Node Registration, [57](#)
vCenter Domain Creation, [408–410](#)
VPC Explicit Protection Group, [202](#)

X-Y-Z

XML (Extensible Markup Language), [103](#)
zAny, [364–365, 589](#)
ZeroMQ, [92, 243](#)
zero-penalty forwarding decision, [248](#)
zero-trust security, [14–15, 151, 600](#)



Connect, Engage, Collaborate

The Award Winning Cisco Support Community

Attend and Participate in Events

Ask the Experts

Live Webcasts

Knowledge Sharing

Documents



DOCUMENTS

Blogs

Videos

Top Contributor Programs

Cisco Designated VIP

Hall of Fame

Spotlight Awards

Multi-Language Support

<https://supportforums.cisco.com>

Exclusive Offer – 40% OFF

Cisco Press Video Training

livelessons®

ciscopress.com/video

Use coupon code CPVIDEO40 during checkout.



Video Instruction from Technology Experts



Advance Your Skills

Train Anywhere

Learn

ADVANCE YOUR SKILLS

Get started with fundamentals,
become an expert, or get certified.

TRAIN ANYWHERE

Train anywhere, at your
own pace, on any device.

LEARN

Learn from trusted author
trainers published by Cisco Press.

Try Our Popular Video Training for FREE!

ciscopress.com/video

Explore hundreds of **FREE** video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

Cisco Press

ciscopress.com/video

ALWAYS LEARNING

PEARSON



REGISTER YOUR PRODUCT at CiscoPress.com/register
Access Additional Benefits and SAVE 35% on Your Next Purchase

- Download available product updates.
- Access bonus material when applicable.
- Receive exclusive offers on new editions and related products.
(Just check the box to hear from us when setting up your account.)
- Get a coupon for 35% for your next purchase, valid for 30 days.
Your code will be available in your Cisco Press cart. (You will also find it in the Manage Codes section of your account page.)

Registration benefits vary by product. Benefits will be listed on your account page

under Registered Products.

CiscoPress.com – Learning Solutions for Self-Paced Study, Enterprise, and the Classroom

Cisco Press is the Cisco Systems authorized book publisher of Cisco networking technology, Cisco certification self-study, and Cisco Networking Academy Program materials.

At CiscoPress.com you can

- Shop our books, eBooks, software, and video training.
- Take advantage of our special offers and promotions (ciscopress.com/promotions).
- Sign up for special offers and content newsletters (ciscopress.com/newsletters).
- Read free articles, exam profiles, and blogs by information technology experts.
- Access thousands of free chapters and video lessons.

Connect with Cisco Press – Visit CiscoPress.com/community

Learn about Cisco Press community events and programs.



Cisco Press

ALWAYS LEARNING

PEARSON

Appendix C

Memory Tables

Chapter 3

Table 3-3 Basic Configuration Parameters for Fabric Initialization

C Configuration Parameter	Description
	A user-friendly name for the fabric. If no name is entered, ACI uses the name ACI Fabric1.
	A numeric identifier between 1 and 128 for the ACI fabric. If no ID is entered, ACI uses 1 as the fabric ID.

	A self-explanatory parameter whose valid values are 1 through 9. The default value is 3 for three APICs. If the intent is to add additional APICs to the fabric in the future, select 3 and modify this parameter when it is time to add new APICs.
	A parameter that determines the unique pod ID to which the APIC being configured is attached. When ACI Multi-Pod is not being deployed, use the default value 1.
	An APIC added to a fabric solely to aid in fabric recovery and in reestablishing an APIC quorum during a prolonged outage. If the APIC being initialized is a standby APIC, select Yes for this parameter.
	The unique ID number for the APIC being configured. Valid values are between 1 and 32. The first three active APICs should always be assigned IDs between 1 and 3. Valid node ID values for standby APICs range from 16 to 32.
	The unique APIC hostname.

The TEP pool assigned to the seed pod. A **TEP pool** is a subnet used for internal fabric communication. This subnet can potentially be advertised outside ACI over an IPN or ISN or when a fabric is extended to virtual environments using the AVS or AVE. TEP pool subnets should ideally be unique across an enterprise environment. Cisco recommends that TEP pool subnet sizes be between /16 and /22. TEP pool sizes *do* impact pod scalability, and use of /16 or /17 ranges is highly advised. Each pod needs a separate TEP pool. However, during APIC initialization, the TEP pool assigned to the seed pod (Pod 1) is what should be entered in the initialization wizard because all APICs in Multi-Pod environments pull their TEP addresses from the Pod 1 TEP pool.

The VLAN ID used for control communication between ACI fabric nodes (leaf switches, spine switches, and APICs). The **infrastructure VLAN** is also used for extending an ACI fabric to AVS or AVE virtual switches. The infra VLAN should be unique and unused elsewhere in the environment. Acceptable IDs are 2 through 4094. Because the VLAN may need to be extended outside ACI, ensure that the selected infrastructure VLAN does not fall into the reserved VLAN range of non-ACI switches.

	The IP address range used for multicast within a fabric. In ACI Multi-Site environments, the same range can be used across sites. If the administrator does not change the default range, 225.0.0.0/15 will be selected for this parameter. Valid ranges are between 225.0.0.0/15 and 231.254.0.0/15. A prefix length of 15 must be used.
	Addresses assigned to OOB LOM ports for access to the APIC GUI. These ports are separate from the IMC ports.
	A parameter that determines whether to enforce the use of passwords of a particular strength for all users. The default behavior is to enforce strong passwords.

Table 3-4 Fabric Node Discovery States

S t a t e	Description
Detected	The node has been detected, but a node ID has not yet been assigned by an administrator in the Fabric Membership view.
Unassigned	

	An administrator has prestaged a switch activation by manually mapping a switch serial number to a node ID, but a switch with the specified serial number has not yet been detected via LLDP and DHCP.
	The node has been detected, and the APICs are in the process of mapping the specified node ID as well as a TEP IP address to the switch.
	The node is a Cisco switch, but it is not supported or the firmware version is not compatible with the ACI fabric.
	The node has been discovered and activated, but a user disabled or decommissioned it. The node can be reenabled.
	An ACI administrator has put the switch into maintenance mode (graceful insertion and removal).
	The node has been discovered and activated, but it is not currently accessible. For example, it may be powered off, or its cables may be disconnected.
	The node is an active member of the fabric.

Table 3-5 Import Types

Import Type	Definition
Merge	
Replace	

Table 3-6 Import Mode

Import Mode	Definition
Best Effort	
Atomic	

Chapter 4

Table 4-3 Fault Severity Levels Users May See in the Faults Page

Description
o
d
e

A service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service, and its capability must be restored.

A service-affecting condition that requires urgent corrective action. For example, this severity could indicate a severe degradation in the capability of the managed object and that its full capability must be restored.

A non-service-affecting fault condition that requires corrective action to prevent a more serious fault from occurring. For example, this severity could indicate that the detected alarm condition is not currently degrading the capacity of the managed object.

A potential or impending service-affecting fault that currently has no significant effects in the system. An action should be taken to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.

A basic notification or informational message that is possibly independently insignificant.

A notification that the underlying condition for a fault has been removed from the system and that the fault will be deleted after a defined interval or after being acknowledged by an administrator.

Table 4-5 Fault Lifecycle Phases

SDescription tate	
	The initial state of a fault, when a problematic condition is first detected. When a fault is created, the soaking interval begins.
	If a fault condition in the Soaking state is resolved at the end of the soaking interval, the fault enters the Soaking-Clearing state. The fault then stays in this state for the clearing interval. During the clearing interval, if the condition reoccurs, the fault transitions back to Soaking. If not, the fault transitions to the Retaining state.

SDescription

t
a
t
e

If a fault condition in the Soaking state is not resolved by the end of the soaking interval, it transitions to the Raised state and can have its severity raised. This state suggests the existence of an active problem in the network. Faults in the Raised state remain in this state until the condition is resolved.

When an administrator addresses a fault condition in the Raised state or when a condition is somehow removed from the system, the fault transitions to the Raised-Clearing state. The clearing interval then begins, and if the condition does not reoccur within this interval, the fault transitions to the Retaining state. If the condition does return within the clearing interval, the fault transitions back to the Raised state.

S Description t a t e	
A fault in the Raised-Clearing or Soaking-Clearing state pertaining to a condition that has been absent within the system for the duration of the clearing interval transitions to the Retaining state with the severity level cleared. The retention interval then begins, and the fault remains in the Retaining state for the length of the interval. The fault is deleted either if the condition does not reoccur in this interval or if an administrator acknowledges the fault. If the fault condition reoccurs during the retention interval, a new fault is generated and placed in the Soaking state. The retention interval is generally lengthy, and the goal of this timer is to ensure that administrators are aware of fault conditions that occur in ACI.	

Table 4-6 Fault Lifecycle Timers

T Description i m e r	
This timer counts the period of time between the system detecting the resolution of a fault condition and the time	

	when the fault severity is set to cleared. This interval refers to the time between the Soaking-Clearing and Retaining fault states. The range for this setting is 0 to 3600 seconds. The default is 120 seconds.
	This timer counts the period of time between the system setting the fault severity to cleared and the time when the fault object is deleted. This interval refers to the time between the Retaining fault state and when the fault is deleted. The range for this setting is 0 to 31536000 seconds. The default is 3600 seconds.
	This timer counts the period of time between ACI creating a fault with the initial severity and the time when it sets the fault to the target severity. This interval refers to the time between the Soaking and Raised fault states. The range for this setting is 0 to 3600 seconds. The default is 120 seconds.

Table 4-7 Classes of Monitoring Policies

M	Description
on	
ito	
rin	
g	
Po	
lic	
y	
Cl	
as	

**S
Na
m
e**

	<p>A class of policies that deals with monitoring of infra objects, which includes monitoring of VMM domains, access ports, and external fabric connectivity. Navigate to Fabric > Access Policies > Policies > Monitoring to configure monitoring policies of the monInfraPol class. By default, all infra objects point to the monInfraPol monitoring policy called default. The DN for this default infra monitoring object is uni/infra/moninfra-default.</p>
	<p>A class of policies that deals with monitoring of fabric objects, which includes monitoring of fabric uplinks. Navigate to Fabric > Fabric Policies > Policies > Monitoring to configure monitoring policies of the monFabricPol class. By default, all fabric objects point to the monFabricPol monitoring policy called default. The DN for this default fabric monitoring policy is uni/fabric/monfab-default.</p>
	<p>A policy class that has a global fabricwide scope and deals with monitoring of objects such as the APIC controllers and fabric nodes. The policies configured in this class are also used when there is no corresponding policy under the more specific infra or tenant scopes. Navigate to Fabric > Fabric Policies > Policies > Monitoring > Common Policy to modify the common</p>

	monitoring policy. The DN for the common monitoring policy is uni/fabric/moncommon.
	A class of policies that deals with monitoring of tenant objects. Navigate to Tenants, select a tenant, and double-click Policies and then Monitoring to configure monitoring policies of the monEPGPol class. By default, all tenant objects point to the monEPGPol monitoring policy called default. The DN for this default tenant monitoring policy is uni/tn-common/monepg-default. This DN refers to a monitoring policy that resides in a tenant called common. Custom tenant-specific monitoring policies can be created and assigned to tenant objects, if desired.

Chapter 6

Table 6-6 Types of Interface Policy Groups in ACI

Interface Description	Policy Group Type
	Fully reusable interface configuration templates used for individual (non-aggregated) non-fabric ports on a leaf switch.

**Interface
Policy
Group
Type**

	A single-switch port channel configuration template that can be applied to non-fabric ports on a leaf switch.
	A vPC configuration template used to create a port aggregation across two switches that are in the same vPC domain.
	Where an administrator reuses PC or VPC interface policy groups across multiple leafs or vPC domains, an override policy group can override the settings applied on an individual leaf or vPC domain.
	Some ACI switches support breaking out high-bandwidth ports into lower-bandwidth ports using breakout cabling. This enables configuration of high-bandwidth ports for breakouts.

Interface Description	Policy Group Type
	A fully reusable interface policy group that allows the selection of an FC interface policy and AAEP for connectivity to SAN-accessing servers or a Fibre Channel Forwarder (FCF).
	A pseudo-reusable FC port channel interface policy group that allows the selection of an FC interface policy, a port channel policy, and an AAEP for connectivity to SAN-accessing servers or an FCF.

Table 6-7 Types of Interface Policies Available in ACI

Interface Description of Settings	Policy Type
	Determines a port link speed, auto-negotiation status, forward error correction (FEC), and link debounce

interval.

Allows the creation of policies that enable or disable CDP.

Allows the creation of policies that enable or disable LLDP.

Allows the creation of NetFlow monitors, NetFlow records, or NetFlow exporters for traffic and flow data collection at the interface level.

Enables the creation of policies involving port aggregations, such as Link Aggregation Control Protocol (LACP) and static port channels. Additional options, including MAC pinning and explicit failover order, are available for virtual environments.

Allows the creation of policies that enable BPDU Guard, BPDU Filtering, or both.

Enables the creation of policies that can prevent traffic disruptions on physical interfaces caused by a broadcast, multicast, or unknown unicast traffic storm.

	Allows the creation of policies that enable or disable <i>MisCabling Protocol (MCP)</i> , which is a loop-prevention protocol in ACI. MCP can be applied on both physical Ethernet interfaces and port channel interfaces. MCP needs to be enabled globally for MCP interface policies to be applied.
	Control Plane Policing (CoPP) interface policies protect ACI switches by setting limits on the number of packets per second the switch may process in CPU when received on a link. CoPP policies are applied on a per-protocol basis.
	L2 interface policies govern policies related to VLAN scopes, Q-in-Q encapsulation, and Reflexive Relay functionality. Later chapters address these policies.

Table 6-10 Most Commonly Deployed Switch Policies in ACI

S	Description of Settings
wi	
tc	
h	
P	
o	
l	
i	
c	
y	

Enables the modification of switch Control Plane Policing (CoPP) profiles to allow a more lenient or more strict profile compared to the default CoPP switch profile. If the predefined CoPP profiles are not sufficient, a custom CoPP switch profile can be configured and allocated to switches.

Enables the configuration of global IPv4 and IPv6 Bidirectional Forwarding Detection (BFD) policies in the fabric to provide subsecond failure detection times in the forwarding path between ACI switches.

Allows the configuration of NetFlow timers that specify the rate at which flow records are sent to the external collector.

This policy provides different scalability options, including the following:

- **Dual Stack:** Provides scalability of up to 12,000 endpoints for IPv6 configurations and up to 24,000 endpoints for IPv4 configurations.

High LPM: Provides scalability similar to Dual Stack except that the longest prefix match (LPM) scale is 128,000, and the policy scale is 8000.

IPv4 Scale: Enables systems with no IPv6 configurations to increase scalability to 48,000 IPv4 endpoints.

High Dual Stack: Provides scalability of up to 64,000 MAC endpoints and 64,000 IPv4 endpoints. IPv6 endpoint scale can be 24,000/48,000, depending on the switch hardware model.

Table 6-12 Access Policy Profiles and Selectors

O Defin it on b j e c t N a m e	

	An interface profile is a collection of interface mappings that gets bound to switch IDs through its association with one or more switch profiles.
	An interface selector is a child object of an interface profile that ties an interface policy group to one or more port IDs. Since switch associations are determined by switch profiles and not interface profiles, interface selectors only determine port ID associations and not the list of switches to which the interface policy groups should be assigned.
	A switch profile is a collection of switch policy group-to-node ID mappings that binds policy to switch IDs using switch selectors. Switch profiles reference interface profiles and deploy the port configurations defined in the interface profiles to switches to which the switch profile is bound. There are two types of switch profiles: leaf profiles and spine profiles.
	A switch selector is a child object of a switch profile that associates a switch policy group to one or more node IDs.

Chapter 7

Table 7-3 Common Control Settings for ACI Port Channel Configuration

C Description on tr ol Se tti n g

	This setting enables fast select for hot standby ports. Enabling this feature makes possible the faster selection of a hot standby port when the last active port in the port channel is going down.
	This setting ensures optimal failover of links in an LACP port channel if the port channel or virtual port channel configured with this setting connects to Nexus devices.
	With this setting configured, LACP suspends a bundled port if it does not receive LACP packets from its peer port. When this setting is not enabled, LACP moves such ports into the Individual state.
	With this setting enabled, bidirectional traffic is forced to use the same physical interface, and each physical interface in the port channel is effectively mapped to a set of flows. When an administrator creates a policy with Symmetric Hashing enabled, ACI exposes a new field for selection of a hashing algorithm.

Chapter 9

Table 9-2 Customizable Settings for an EIGRP Address Family Context Policy

Co Description	
n	The interval the border leaf waits after an EIGRP query is sent before declaring a stuck in active (SIA) situation and resetting the neighborship. The default is 3 minutes.
fi	The administrative distance (AD) for external EIGRP routes. The default AD for external routes is 170.
gu	
ra	
ti	
on	
Pa	
ra	
m	
et	
er	

The maximum number of equal-cost multipathing (ECMP) next-hop addresses EIGRP can install into the routing table for a prefix. The default is eight paths.

EIGRP calculates its metric based on bandwidth and delay along with default K values. However, the original 32-bit implementation cannot differentiate interfaces faster than 10 Gigabit Ethernet. This original implementation is called the classic, or narrow, metric. To solve this problem, a 64-bit value with an improved formula was introduced for EIGRP; this is called the wide metric. Valid values for metric style are narrow metric and wide metric. The default is the narrow metric.

Table 9-5 Configuration Parameters in BGP Peer Connectivity Profiles

C Description
**o
n
fi
g
u
ra
ti
o
n
P
ar
a
m
et
er**

	Allows ACI to receive routes from eBGP neighbors when the routes have the ACI BGP AS number in the AS_PATH. This option is valid only for eBGP peers.
	Allows ACI to overwrite a remote AS in the AS_PATH with the ACI BGP AS. This is typically used when performing Transit Routing from an eBGP L3Out to another eBGP L3Out with the same AS number. Otherwise, an eBGP peer device may not accept the route from ACI because of AS_PATH loop prevention. When this option is enabled, Disable Peer AS Check also needs to be enabled. This option is valid only for eBGP peers.

	Allows ACI to advertise a route to the eBGP peer even if the most recent AS in the <code>AS_PATH</code> of the route is the same as the remote AS for the eBGP peer. This option is valid only for eBGP peers.
	Allows ACI to update the next-hop address when advertising a route from an eBGP peer to an iBGP peer. By default, route advertisement between iBGP peers keeps the original next-hop address of the route, and the one between eBGP peers always updates the next-hop address with a self IP address.
	When enabled, allows ACI L3Out to advertise routes with a BGP Community attribute, such as <code>AS2>NN</code> format. Otherwise, the BGP Community attribute is stripped when routes are advertised to the outside.
	When enabled, allows ACI L3Out to advertise routes along with the BGP Extended Community attribute, such as <code>RT:AS2>NN</code> , <code>RT:AS4>NN</code> , and so on. Otherwise, the BGP Extended Community attribute is stripped when routes are advertised to the outside.
	When configured, allows the BGP peering to use MD5 authentication on the BGP TCP session. The password can be reset by right-clicking the BGP peer connectivity profile and selecting Reset Password.

	Sets the maximum count for the Allow Self AS option under BGP controls.
	Enables BFD on the BGP neighbor.
	Provides an alternative to increasing the eBGP multihop TTL in cases where there is a security concern about increasing TTL unnecessarily. For eBGP peering, BGP checks whether the neighbor IP is on the same subnet as any of its local interfaces to see if the neighbor IP is directly connected. If it is not, BGP automatically assumes that the TTL needs to be larger than 1. Hence, when BGP is peering via loopbacks with directly connected routers, the BGP peering is rejected without the eBGP Multihop TTL being set to 2 or larger, even though TTL 1 is technically enough.
	Sets the default value of a Cisco proprietary BGP path attribute weight on all the routes learned from the border leaf by the configured peer.
	In outgoing eBGP route updates to this neighbor, removes all private AS numbers from the AS_PATH when the AS_PATH has only private AS numbers. This option is not applied if the neighbor remote AS is in the AS_PATH.

	<p>In outgoing eBGP route updates to this neighbor, removes all private AS numbers from the AS_PATH, regardless of whether a public AS number is included in the AS_PATH. This feature does not apply if the neighbor remote AS is in the AS_PATH. To enable this option, Remove Private AS needs to be enabled.</p>
	<p>In outgoing eBGP route updates to this neighbor, replaces all private AS numbers in the AS_PATH with ACI local AS, regardless of whether a public AS or the neighbor remote AS is included in the AS_PATH. To enable this option, Remove All Private AS needs to be enabled.</p>
	<p>Defines an action to take when the number of received prefixes from this neighbor exceeds the configured maximum number. This option is activated by attaching a BGP peer prefix policy to the BGP peer connectivity profile.</p>

	<p>Disguises the ACI BGP ASN with the configured local ASN to peer with a particular neighbor. When this feature is used, it looks like there is one more ASN (local AS) between the ACI BGP AS and the external neighbor. Hence, the neighbor peers with the configured local ASN instead of the real ACI BGP ASN. In such situations, both the local ASN and the real ACI BGP ASN are added to the AS_PATH of routes advertised to the neighbor. The local ASN is also prepended to routes learned from the neighbor.</p>
	<p>Allows granular control over how the local ASN and the fabric ASN appear in the AS_PATHs of routes advertised to external routers or received by the fabric.</p> <p>The no-prepend option prevents ACI from prepending the local ASN in the AS_PATHs of routes learned from this neighbor.</p> <p>The no-prepend, replace-as option allows ACI to add only a local ASN, instead of both a local ASN and a real ACI BGP ASN, to the AS_PATHs of routes advertised to this neighbor on top of the no-prepend option effect.</p> <p>The no-prepend, replace-as, dual-as option allows the neighbor to peer with both a local ASN and a real ACI BGP ASN on top of the no-prepend and replace-as option effect.</p>

	Enables a BGP session with a peer to be turned off or on.
	Allows application of a route profile to a specific BGP neighbor.

Table 9-7 Components of a Route Profile

Component	Description
Route Profile	The route profile type is specific to ACI. There are two route profile types. One type, Match Prefix AND Routing Policy, combines prefixes from the component that the route profile is associated with and the match criteria configured in the route profile. Components that route profiles can be associated to include bridge domains, bridge domain subnets, L3Outs, L3Out EPGs, and L3Out EPG subnets. The other type, Match Routing Policy Only, only matches routes based on criteria configured in the route profile and ignores prefixes from the components with which the route profile is associated.

	<p>In a sense, each entry in a route profile includes two context options: Order and Action. Order is equivalent to a sequence number in a normal route map with the caveat that some route profiles merge internal route maps of components with statements explicitly entered by administrators, changing the actual applicable sequence of rules. Action consists of permit or deny and is equivalent in function to permit or deny in a normal route map.</p>
	<p>Route profile match rules are similar to match clauses in route maps. Clauses ACI can match against include prefixes, community attributes, and regular expressions.</p>
	<p>Set rules are equivalent to set clauses in a route map. ACI can set parameters such as community attributes, weight, OSPF types, and AS_PATH.</p>

Chapter 10

Table 10-2 Bridge Domain Settings for ACI Layer 2 Extension to Non-ACI Switches

B Required Setting for Property and Justification

D

P
r
o
p
e
r
t
y

The Forwarding field only appears when a bridge domain is first configured. Its default value, Optimized, automatically sets the Unicast and ARP parameters. To enable customization of forwarding settings to values that enable Layer 2 extension, select the Custom option.

This field applies to unicast traffic destined to an endpoint whose MAC address cannot be found in the ACI endpoint table.

The forwarding options available for the L2 Unknown Unicast parameter are Flood and Hardware Proxy. When endpoints directly attach to leaf switches and ACI is the default gateway for the BD, hardware proxy forwarding is preferred because it allows for a reduction in flooding within the fabric. However, when some endpoints associated with a bridge domain as well as the default gateway for the BD subnet(s) reside outside the fabric, the ACI spine proxy forwarding behavior can lead to suboptimal learning on non-ACI switches outside the fabric. For this reason, the L2 Unknown Unicast setting needs to be set to Flood to accommodate any endpoints behind the Layer 2 extension until default gateways are moved into the fabric and unicast routing is enabled on the BD.

By default, IGMP snooping is enabled on bridge domains. The IGMP snooping feature snoops the IGMP membership reports and leave messages and forwards them to the IGMP router function only when necessary. When a leaf receives traffic for a multicast group that is unknown, this traffic is considered unknown Layer 3 multicast, and the L3 Unknown Multicast Flooding setting determines how the traffic is forwarded. The two options for this setting are Flood and Optimized Flood. When Flood is selected, traffic destined to unknown multicast groups is flooded on the ingress switch and any border leafs on which the BD is active. When Optimized Flood is selected, traffic for the unknown multicast group is forwarded to the multicast router ports only.

When the ARP Flooding parameter is enabled, ARP requests with a broadcast destination MAC address are flooded in the bridge domain. If this option is disabled and the fabric has already learned the destination endpoint, it unicasts the ARP request to the destination. If this option is disabled and the fabric has *not* learned the destination endpoint, it uses ARP gleaning to identify the destination endpoint. When unicast routing is disabled, ARP traffic is always flooded, even if the ARP Flooding parameter has been disabled on the BD.

Enabling ARP Flooding ensures that ACI behaves much like traditional networks and allows non-ACI switches behind a Layer 2 extension to proactively learn endpoints residing in the fabric. This, by itself, should be sufficient justification for its use during migrations into ACI. There is one other compelling use case for enabling the ARP

Flooding parameter that relates to silent hosts. Remember from [Chapter 8, “Implementing Tenant Policies,”](#) that ARP gleaning detects silent hosts by prodding them into communicating on the network, but in the rare case that the silent host moves elsewhere without sending a GARP packet into the network, ACI continues to think that the endpoint details it learned prior to the endpoint move are accurate. In this case, if ARP Flooding has been disabled, the ACI leaf continues to unicast ARP requests that are destined to the silent host to the old location until the IP endpoint ages out. On the other hand, with ARP Flooding enabled, ACI floods all ARP requests with broadcast destination MAC addresses. When the silent host receives the ARP request, it responds to the ARP request, prompting ACI nodes to update the endpoint table accordingly. Even though the issue of silent hosts is not specifically related to Layer 2 extension, this example should help illuminate why the ARP Flooding parameter can help alleviate some corner-case endpoint learning issues.

This parameter primarily addresses forwarding of traffic types not covered by the other settings mentioned in this table, such as broadcast, L2 multicast, and link-local traffic. There are three configuration options for the Multi Destination Flooding property:

- **Flood in BD:** Sends a packet to all ports in the same bridge domain.

- **Drop:** Drops a packet and never sends it to any other ports.
- **Flood in Encapsulation:** Sends a packet to all ports in the same VLAN encapsulation. If there is a one-to-one relationship between encapsulations and EPGs, this setting effectively limits flooding to each EPG.

Note that while Flood in Encapsulation does enable Layer 2 extension and is an option in some deployments, there are more caveats that require careful consideration when using this option for migrations. The Flood in BD option, which is the default setting for the L3 Unknown Multicast Flooding bridge domain property, remains the most ideal setting for Layer 2 extension.

Table 10-3 Comparison Between Bridge Domain Extension and EPG Extension

Co mp ari son	Extend EPG	Extend Bridge Domain
------------------------	------------	----------------------

Cri teri a		
Use cases		Extend a bridge domain out the fabric or extend a tenant subnet of the bridge domain out the fabric; migrate VLANs into ACI with intra-VLAN policy enforcement applied at the time of migration
Configration	Statically assign a port to an EPG (static binding under EPG or direct assignment to an AAEP)	
Domain type applicable		External bridged domain
	Endpoints connected to non-	

	ACI switches placed in the same EPG (VLAN) as directly attached endpoints	
	External endpoints are seen as an internal EPG, and the same principles apply.	An external endpoint is placed under an external EPG (Layer 2 EPG). Policy is applied between internal EPGs and a Layer 2 EPG.
	ACI learns both MAC and IP addresses. (IP addresses are only learned if unicast routing is enabled at the BD level.)	ACI learns both MAC and IP addresses. (IP addresses are only learned if unicast routing is enabled at the BD level.)

Chapter 11

Table 11-2 vSphere Teaming and Failover Settings

Description
Teaming

Specifies one of two ways with which a virtual switch can detect network uplink failures. The first, Link Status Only, relies on the operational state of the link. The second option, Beacon Probing, sends probes into the network through its uplinks to see if other uplinks receive the probes. If an uplink is unable to receive the transmitted probes, it is deemed to have suboptimal connectivity. Use of beacon probing is very uncommon because it requires at least three uplinks to allow the virtual switch to effectively determine which of the uplinks has failed. The beacon probing option should never be used in combination with port channeling.

When set to Yes, prompts the virtual switch repinning a virtual machine to a different uplink following an uplink failure to send a Reverse ARP (RARP) packet into the network in the hope that upstream switches update their CAM tables faster.

When all interfaces in the Active Uplinks list have been determined to be non-operational and virtual machines and VMkernel interfaces have been pinned to interfaces in the Standby list, a fallback setting of Yes specifies whether the virtual switch should fall back to interfaces in the Active uplinks list if they become available.

Specifies how traffic should be rerouted when an adapter fails. There are three possible adapter states that can be configured in the teaming and failover page: Active

Uplinks, Standby Uplinks, and Unused Uplinks. Active uplinks actively forward traffic, while standby uplinks are only used if all active uplinks fail. An uplink that has been added to the Unused Uplinks list is never used for traffic in a port group, even if both the active and standby uplinks fail.

Chapter 12

Table 12-2 Components of a Device Package

De vi c e Pa ck ag e Co m po ne nt	Description
	An XML file that defines the following: <ul style="list-style-type: none">■ Device properties:

- **Model:** Model of the device
- **Vendor:** Vendor of the device
- **Version:** Software version of the device
- Functions provided by the device
- Interfaces and network connectivity information for each function
- Device configuration parameters

	Configuration parameters for each function
	A Python script that allows the APICs to interact with the device. The device script maps APIC events to function calls. A device package can contain multiple device scripts. A device script can interface with services devices via REST, SSH, or any similar mechanism.
	An L4-L7 configuration template that includes configuration values for deployment to L4-L7 services devices. When a vendor creates a device package, it typically defines a number of function profiles corresponding with the various functions provided by the services device. The vendor populates default values for a number of parameters within each function profile. Administrators can modify most of the default values to suit their requirements.
	A configuration file that specifies parameters that are required by a device. This configuration can be shared by one or more service graphs.

Table 12-3 Configuration Options in the Create L4-L7 Devices Page

Description

Co nfi gur ati on

Three options are available in this drop-down box:

- ADC

- Firewall

- Other

Possible options available for this parameter include the following:

- **Physical:** Bare-metal servers, physical appliances, or non-VMM integrated virtual environments
- **Virtual:** A VM integrated using a VMM integration

This configuration option is part of the service VM orchestration solution and enables APICs to trigger an instantiation of a VM template in vCenter.

This option specifies the context-awareness of the device, which can be one of the following:

- **Single:** The device cluster cannot be shared across multiple tenants of a given type that are hosted on the provider network. You must give the device cluster to a specific tenant for a given user.
- **Multiple:** The device cluster can be shared across multiple tenants of a given type that you are hosting

	<p>on the provider network. For example, two hosting companies might share the same device.</p>
	<p>When defining a load balancer as a Layer 4 to Layer 7 services device, the Context Aware parameter is not used and can be ignored.</p>
	<p>This option refers to deployment modes, including GoThrough and GoTo for routed firewalls and transparent firewalls, respectively.</p>

Chapter 15

Table 15-2 Predefined Roles in ACI

Role Name	Description
Authz	Aids in configuring authentication, authorization, accounting, and import/export policies
Device Manager	Manages devices and their configurations

	Enables administration and configuration of access policies
	Provides full access to an ACI fabric
	Enables administration and configuration of fabricwide settings and also firmware management
	Allows users to configure L4-L7 network service insertion and orchestration
	Grants access to the parameters governing the configuration of external L4-L7 devices
	Provides network operator privileges to an ACI fabric to allow for monitoring and troubleshooting functionality in ACI
	Provides read-only visibility into an ACI fabric
	When assigned to a limited security domain, allows configuration of most attributes inside a tenant but does not allow changes to fabricwide settings that can potentially impact other tenants

	Allows the configuration of external connectivity, such as L3Outs, for ACI tenants; a subset of the tenant-admin role
	Grants access to ACI integrations with virtualization environments such as Microsoft Hyper-V, OpenStack, and VMware vSphere

Table 15-6 Configuration Parameters for LDAP Providers

C on fig u ra ti o n P ar a m et er	Description
	ACI allows administrators to reference an LDAP server by using either its IP address or DNS address.

	This is the service port number for the LDAP service. The range is from 1 to 65535. The default is 389.
	This is a string referencing an account on an LDAP server that is able to query at least a portion of the LDAP directory hierarchy. This account should ideally be a system account with a non-expiring password. In non-production environments leveraging LDAP servers with anonymous bind capabilities, this field can be left empty. LDAP server administrators need to provide ACI administrators the exact Bind DN string.
	This is a string referencing the container and subtree under which ACI is able to execute queries for matching users using the bind account. LDAP server administrators need to provide ACI administrators the exact Base DN string.
	This is the password of the LDAP account specified in the Bind DN field.
	This is the number of seconds ACI nodes wait for a response from the LDAP provider server. The acceptable range is from 5 to 60 seconds. The default is 30 seconds.

	<p>This is the number of times ACI automatically retries login attempts for a single authentication submission. The acceptable range is from 1 to 5 retries. The default is 1.</p>
	<p>This checkbox allows administrators to enforce SSL-based connections with the LDAP provider.</p>
	<p>Acceptable values for this option are Permissive and Strict. Permissive certificate checking relaxes requirements around certificate validation, making it an ideal option in deployments that use self-signed certificates. Strict certificate validation is ideal in production environments.</p>
	<p>ACI determines the level of user authorization from the Attribute field. The two most common values for this field are memberOf and CiscoAVPair. When using the memberOf option, configuration of LDAP group map rules is mandatory.</p>
	<p>Filters defines how ACI queries an LDAP schema and interprets the existence of a user. The LDAP provider configuration page provides three options for the Filter Type parameter: Default, Microsoft AD, and Custom.</p>

	This is a custom filter value.
	This is the management EPG (in-band or out-of-band) from which ACI should source requests to the LDAP server.
	This parameter can be set to either Enabled or Disabled. When it is enabled for an LDAP provider, the APICs periodically attempt to execute login attempts against the LDAP provider to verify that the LDAP service is alive on the server. When enabled, ACI asks administrators to additionally enter a username and password. By default, Server Monitoring is set to Disabled. Server monitoring checks are exclusive to APICs. To enable monitoring checks that leafs and spines are also able to perform, use of the Ping Check option under the AAA Policy view is more common.

Table 15-7 Settings on the AAA Policy Page

Description
Setting

There are two acceptable values for this setting. Assign Default Role ensures that any remotely authenticated user with a bad or missing Cisco AV pair gets assigned to the common security domain using the read-all role and the privilege type Read. No Login, on the other hand, ensures that such users cannot log in to the fabric. The default value for this setting is No Login.

ACI performs ICMP health checks against AAA providers. The Ping Check setting can be set to either True or False. ACI continues to run ICMP health checks against all AAA providers, regardless of the value chosen. If Ping Check is set to True, ACI removes inaccessible providers from the authentication process and authenticates against operational providers instead. If ICMP traffic cannot reach AAA servers due to firewall rules, the Ping Check setting should be set to False to ensure that ACI continues to authenticate against all servers, regardless of the result of ICMP health checks.

This setting governs the login domain ACI uses when a user does not select a domain when logging in to the fabric. It also determines the login domain used when a user attempts to log in to the fabric by using the DefaultAuth domain. You can select Local, LDAP, RADIUS, TACACS+, RSA, or SAML for Default Authentication Realm. Local is selected by default. When you select a setting other than Local, an additional Login Domain field appears, allowing selection of the intended domain.

ACI comes with a preconfigured login domain called fallback that is set to local authentication by default. The Fallback Check setting, which can be set to True or False, enables or disables reliance on the AAA provider ICMP health check for activation of the fallback domain. If fallback check is set to True and the configured AAA providers respond to ICMP traffic but are unable to authenticate users, the fallback login domain will be unavailable, and users may remain locked out of the fabric. For this reason, Fallback Check is often kept at its default value of False.

This parameter allows users to specify the authentication method for console logins to ACI nodes. By default, it is set to Local. Other valid options are LDAP, RADIUS, TACACS+, and RSA. When you select a setting besides Local, ACI exposes an additional field for you to specify the login domain.

Appendix D

Memory Tables Answer Key

Chapter 3

Table 3-3 Basic Configuration Parameters for Fabric Initialization

C	Description
on	Configuration parameter
fi	Configuration parameter
g	Configuration parameter
ur	Configuration parameter
at	Configuration parameter
io	Configuration parameter
n	Configuration parameter
Pa	Configuration parameter
ra	Configuration parameter
m	Configuration parameter
et	Configuration parameter
er	Configuration parameter

Fabric Name	A user-friendly name for the fabric. If no name is entered, ACI uses the name ACI Fabric1.
Fabric ID	A numeric identifier between 1 and 128 for the ACI fabric. If no ID is entered, ACI uses 1 as the fabric ID.
Number of active controllers	A self-explanatory parameter whose valid values are 1 through 9. The default value is 3 for three APICs. If the intent is to add additional APICs to the fabric in the future, select 3 and modify this parameter when it is time to add new APICs.
Pod ID	A parameter that determines the unique pod ID to which the APIC being configured is attached. When ACI Multi-ID Pod is not being deployed, use the default value 1.

<p>St an db y</p> <p>Co nt rol ler</p>	<p>An APIC added to a fabric solely to aid in fabric recovery and in reestablishing an APIC quorum during a prolonged outage. If the APIC being initialized is a standby APIC, select Yes for this parameter.</p>
<p>Co nt rol ler ID</p>	<p>The unique ID number for the APIC being configured. Valid values are between 1 and 32. The first three active APICs should always be assigned IDs between 1 and 3. Valid node ID values for standby APICs range from 16 to 32.</p>
<p>Co nt rol ler Na m e</p>	<p>The unique APIC hostname.</p>

Po d	The TEP pool assigned to the seed pod. A TEP pool is a subnet used for internal fabric communication. This subnet can potentially be advertised outside ACI over an IPN or ISN or when a fabric is extended to virtual environments using the AVS or AVE. TEP pool subnets should ideally be unique across an enterprise environment. Cisco recommends that TEP pool subnet sizes be between /16 and /22. TEP pool sizes <i>do</i> impact pod scalability, and use of /16 or /17 ranges is highly advised. Each pod needs a separate TEP pool. However, during APIC initialization, the TEP pool assigned to the seed pod (Pod 1) is what should be entered in the initialization wizard because all APICs in Multi-Pod environments pull their TEP addresses from the Pod 1 TEP pool.
Infra structure (in fra VL VL A N	The VLAN ID used for control communication between ACI fabric nodes (leaf switches, spine switches, and APICs). The infrastructure VLAN is also used for extending an ACI fabric to AVS or AVE virtual switches. The infra VLAN should be unique and unused elsewhere in the environment. Acceptable IDs are 2 through 4094. Because the VLAN may need to be extended outside ACI, ensure that the selected infrastructure VLAN does not fall into the reserved VLAN range of non-ACI switches.

B The IP address range used for multicast within a fabric.
D In ACI Multi-Site environments, the same range can be
M used across sites. If the administrator does not change
ult the default range, 225.0.0.0/15 will be selected for this
ic parameter. Valid ranges are between 225.0.0.0/15 and
as 231.254.0.0/15. A prefix length of 15 must be used.

t
Ad
dr
es
se
s
(G
iP
o)

AP IC OOB Address and Default Gate way	Addresses assigned to OOB LOM ports for access to the APIC GUI. These ports are separate from the IMC ports.
Password Strength	A parameter that determines whether to enforce the use of passwords of a particular strength for all users. The default behavior is to enforce strong passwords.

Table 3-4 Fabric Node Discovery States

State Description	
Unknown	The node has been detected, but a node ID has not yet been assigned by an administrator in the Fabric Membership view.
Undiscovered	An administrator has prestaged a switch activation by manually mapping a switch serial number to a node ID, but a switch with the specified serial number has not yet been detected via LLDP and DHCP.
Discovering	The node has been detected, and the APICs are in the process of mapping the specified node ID as well as a TEP IP address to the switch.
Unsupported	The node is a Cisco switch, but it is not supported or the firmware version is not compatible with the ACI fabric.
Disabled/Decommissioned	The node has been discovered and activated, but a user disabled or decommissioned it. The node can be reenabled.

Maint enanc e	An ACI administrator has put the switch into maintenance mode (graceful insertion and removal).
Inactive	The node has been discovered and activated, but it is not currently accessible. For example, it may be powered off, or its cables may be disconnected.
Active	The node is an active member of the fabric.

Table 3-5 Import Types

Import Type	Definition
Merge	The import operation combines the configuration in the backup file with the current configuration.
Replace	The import operation overwrites the current configuration with the configuration imported from the backup file.

Table 3-6 Import Mode

Definition

I m p o r t M o d e

B	Each shard is imported, but if there are objects within a shard that are invalid, these objects are ignored and not imported. If the version of the configuration being imported is incompatible with the current system, shards that can be imported are imported, and all other shards are ignored.
At	The import operation is attempted for each shard, but if a shard has any invalid configuration, the shard is ignored and not imported. Also, if the version of the configuration being imported is incompatible with the current system, the import operation terminates.

Chapter 4

Table 4-3 Fault Severity Levels Users May See in the Faults Page

Description

M
o
d
e

C	A service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service, and its capability must be restored.
M	A service-affecting condition that requires urgent corrective action. For example, this severity could indicate a severe degradation in the capability of the managed object and that its full capability must be restored.
W	A non-service-affecting fault condition that requires corrective action to prevent a more serious fault from occurring. For example, this severity could indicate that the detected alarm condition is not currently degrading the capacity of the managed object.
I	A potential or impending service-affecting fault that currently has no significant effects in the system. An action should be taken to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.

n g	I A basic notification or informational message that is n possibly independently insignificant.
f o r e d	C A notification that the underlying condition for a fault has I been removed from the system and that the fault will be e deleted after a defined interval or after being a acknowledged by an administrator.

Table 4-5 Fault Lifecycle Phases

S	Description
k i	S The initial state of a fault, when a problematic condition is of first detected. When a fault is created, the soaking a interval begins.

n
g

SIf a fault condition in the Soaking state is resolved at the end of the soaking interval, the fault enters the Soaking-Clearing state. The fault then stays in this state for the clearing interval. During the clearing interval, if the condition reoccurs, the fault transitions back to Soaking. If not, the fault transitions to the Retaining state.

g
-
C
I
e
a
r
i
n
g

RIf a fault condition in the Soaking state is not resolved by the end of the soaking interval, it transitions to the Raised state and can have its severity raised. This state suggests the existence of an active problem in the network. Faults in the Raised state remain in this state until the condition is resolved.

RWhen an administrator addresses a fault condition in the Raised state or when a condition is somehow removed from the system, the fault transitions to the Raised-Clearing state. The clearing interval then begins, and if

the condition does not reoccur within this interval, the fault transitions to the Retaining state. If the condition does return within the clearing interval, the fault transitions back to the Raised state.

L
e
a
r
i
n
g

A fault in the Raised-Clearing or Soaking-Clearing state pertaining to a condition that has been absent within the system for the duration of the clearing interval transitions to the Retaining state with the severity level cleared. The retention interval then begins, and the fault remains in the Retaining state for the length of the interval. The fault is deleted either if the condition does not reoccur in this interval or if an administrator acknowledges the fault. If the fault condition reoccurs during the retention interval, a new fault is generated and placed in the Soaking state. The retention interval is generally lengthy, and the goal of this timer is to ensure that administrators are aware of fault conditions that occur in ACI.

Table 4-6 Fault Lifecycle Timers

Ti m er	Description
Clearing	The clearing timer monitors the duration of a fault condition. If the condition remains active for longer than the clearing interval, the fault transitions to the Retaining state.
Retention	The retention timer monitors the duration of a fault condition while it is in the Retaining state. If the condition remains inactive for longer than the retention interval, the fault is deleted.
Soaking	The soaking timer monitors the duration of a fault condition while it is in the Soaking state. If the condition remains inactive for longer than the soaking interval, a new fault is generated and placed in the Soaking state.

Cl ea rin g Int er va l	This timer counts the period of time between the system detecting the resolution of a fault condition and the time when the fault severity is set to cleared. This interval refers to the time between the Soaking-Clearing and Retaining fault states. The range for this setting is 0 to 3600 seconds. The default is 120 seconds.
Re te nti on Int er va l	This timer counts the period of time between the system setting the fault severity to cleared and the time when the fault object is deleted. This interval refers to the time between the Retaining fault state and when the fault is deleted. The range for this setting is 0 to 31536000 seconds. The default is 3600 seconds.
So ak in g Int er va l	This timer counts the period of time between ACI creating a fault with the initial severity and the time when it sets the fault to the target severity. This interval refers to the time between the Soaking and Raised fault states. The range for this setting is 0 to 3600 seconds. The default is 120 seconds.

Table 4-7 Classes of Monitoring Policies

Description

M on ito rin g Po lic y Cl as s Na m e

m	A class of policies that deals with monitoring of infra objects, which includes monitoring of VMM domains, access ports, and external fabric connectivity. Navigate to Fabric > Access Policies > Policies > Monitoring to configure monitoring policies of the monInfraPol class. By default, all infra objects point to the monInfraPol monitoring policy called default. The DN for this default infra monitoring object is uni/infra/moninfra-default.
m	A class of policies that deals with monitoring of fabric objects, which includes monitoring of fabric uplinks. Navigate to Fabric > Fabric Policies > Policies > Monitoring to configure monitoring policies of the monFabricPol class. By default, all fabric objects point to the monFabricPol monitoring policy called default. The DN for this default fabric monitoring policy is uni/fabric/monfab-default.

	<p>m A policy class that has a global fabricwide scope and deals with monitoring of objects such as the APIC controllers and fabric nodes. The policies configured in this class are also used when there is no corresponding policy under the more specific infra or tenant scopes.</p> <p>on Navigate to Fabric > Fabric Policies > Policies > Monitoring > Common Policy to modify the common monitoring policy. The DN for the common monitoring policy is uni/fabric/moncommon.</p>
	<p>m A class of policies that deals with monitoring of tenant objects. Navigate to Tenants, select a tenant, and double-click Policies and then Monitoring to configure monitoring policies of the monEPGPol class. By default, all tenant objects point to the monEPGPol monitoring policy called default. The DN for this default tenant monitoring policy is uni/tn-common/monepg-default. This DN refers to a monitoring policy that resides in a tenant called common. Custom tenant-specific monitoring policies can be created and assigned to tenant objects, if desired.</p>

Chapter 6

Table 6-6 Types of Interface Policy Groups in ACI

Interface Policy Group Type	Description
Leaf access port policy group	Fully reusable interface configuration templates used for individual (non-aggregated) non-fabric ports on a leaf switch.
Port channel interface policy group	A single-switch port channel configuration template that can be applied to non-fabric ports on a leaf switch.
VPC interface policy group	A vPC configuration template used to create a port aggregation across two switches that are in the same vPC domain.
PC/VPC override policy group	Where an administrator reuses PC or VPC interface policy groups across multiple leafs or vPC domains, an override policy group can override the settings applied on an individual leaf or vPC domain.

Leaf breakout port group	Some ACI switches support breaking out high-bandwidth ports into lower-bandwidth ports using breakout cabling. This enables configuration of high-bandwidth ports for breakouts.
Fibre Channel (FC) interface policy group	A fully reusable interface policy group that allows the selection of an FC interface policy and AAEP for connectivity to SAN-accessing servers or a Fibre Channel Forwarder (FCF).
FC port channel interface policy group	A pseudo-reusable FC port channel interface policy group that allows the selection of an FC interface policy, a port channel policy, and an AAEP for connectivity to SAN-accessing servers or an FCF.

Table 6-7 Types of Interface Policies Available in ACI

Inte rfac e	Description of Settings
Poli cy Type	

Link level	Determines a port link speed, auto-negotiation status, forward error correction (FEC), and link debounce interval.
CDP	Allows the creation of policies that enable or disable CDP.
LLDP	Allows the creation of policies that enable or disable LLDP.
NetFlow	Allows the creation of NetFlow monitors, NetFlow records, or NetFlow exporters for traffic and flow data collection at the interface level.
Port channel	Enables the creation of policies involving port aggregations, such as Link Aggregation Control Protocol (LACP) and static port channels. Additional options, including MAC pinning and explicit failover order, are available for virtual environments.
Spanning Tree	Allows the creation of policies that enable BPDU Guard, BPDU Filtering, or both.
Storm	Enables the creation of policies that can prevent traffic disruptions on physical interfaces caused by a

control	broadcast, multicast, or unknown unicast traffic storm.
MCP	Allows the creation of policies that enable or disable <i>MisCabling Protocol (MCP)</i> , which is a loop-prevention protocol in ACI. MCP can be applied on both physical Ethernet interfaces and port channel interfaces. MCP needs to be enabled globally for MCP interface policies to be applied.
Control Plane Policing (CoPP)	Control Plane Policing (CoPP) interface policies protect ACI switches by setting limits on the number of packets per second the switch may process in CPU when received on a link. CoPP policies are applied on a per-protocol basis.
L2 interface policy	L2 interface policies govern policies related to VLAN scopes, Q-in-Q encapsulation, and Reflexive Relay functionality. Later chapters address these policies.

Table 6-10 Most Commonly Deployed Switch Policies in ACI

Switch Description of Settings

Policy

CoPP	Enables the modification of switch Control Plane Policing (CoPP) profiles to allow a more lenient or more strict profile compared to the default CoPP switch profile. If the predefined CoPP profiles are not sufficient, a custom CoPP switch profile can be configured and allocated to switches.
BFD	Enables the configuration of global IPv4 and IPv6 Bidirectional Forwarding Detection (BFD) policies in the fabric to provide subsecond failure detection times in the forwarding path between ACI switches.
NetFlow node	Allows the configuration of NetFlow timers that specify the rate at which flow records are sent to the external collector.
Forwarding scalability profile	This policy provides different scalability options, including the following:

- **Dual Stack:** Provides scalability of up to 12,000 endpoints for IPv6 configurations and up to 24,000 endpoints for IPv4 configurations.
- **High LPM:** Provides scalability similar to Dual Stack except that the longest prefix match (LPM) scale is 128,000, and the policy scale is 8000.
- **IPv4 Scale:** Enables systems with no IPv6 configurations to increase scalability to 48,000 IPv4 endpoints.
- **High Dual Stack:** Provides scalability of up to 64,000 MAC endpoints and 64,000 IPv4 endpoints. IPv6 endpoint scale can be 24,000/48,000, depending on the switch hardware model.

Table 6-12 Access Policy Profiles and Selectors

O Definition
bj
ec
t

N a m e

In An interface profile is a collection of interface mappings
te that gets bound to switch IDs through its association
rf with one or more switch profiles.

a c e pr o fil e

In An interface selector is a child object of an interface
te profile that ties an interface policy group to one or more
rf port IDs. Since switch associations are determined by
ac switch profiles and not interface profiles, interface
e selectors only determine port ID associations and not
se the list of switches to which the interface policy groups
le should be assigned.

c t or

S A switch profile is a collection of switch policy group-to-
wi node ID mappings that binds policy to switch IDs using
tc switch selectors. Switch profiles reference interface
h profiles and deploy the port configurations defined in
pr the interface profiles to switches to which the switch
o

fil	profile is bound. There are two types of switch profiles: e leaf profiles and spine profiles.
S wi tc h se le ct or	A switch selector is a child object of a switch profile that associates a switch policy group to one or more node IDs.

Chapter 7

Table 7-3 Common Control Settings for ACI Port Channel Configuration

Control Setting	Description
Fast Select	This setting enables fast select for hot standby ports. Enabling this feature makes possible the faster selection of a hot standby port when the last active port in the port channel is going down.

Graceful Convergence	This setting ensures optimal failover of links in an LACP port channel if the port channel or virtual port channel configured with this setting connects to Nexus devices.
Suspension Period	With this setting configured, LACP suspends a bundled port if it does not receive LACP packets from its peer port. When this setting is not enabled, LACP moves such ports into the Individual state.
Symmetric Hashing	With this setting enabled, bidirectional traffic is forced to use the same physical interface, and each physical interface in the port channel is effectively mapped to a set of flows. When an administrator creates a policy with Symmetric Hashing enabled, ACI exposes a new field for selection of a hashing algorithm.

Chapter 9

Table 9-2 Customizable Settings for an EIGRP Address Family Context Policy

Category	Description
None	

ra ti on Pa ra m et er

Ac tiv e Int er va l (m in)	The interval the border leaf waits after an EIGRP query is sent before declaring a stuck in active (SIA) situation and resetting the neighborship. The default is 3 minutes.
Ex ter na l Di st an ce	The administrative distance (AD) for external EIGRP routes. The default AD for external routes is 170.
Int er na	The AD for internal EIGRP routes. The default AD for internal routes is 90.

I Di st an ce	
M ax im um Pa th Li mi t	The maximum number of equal-cost multipathing (ECMP) next-hop addresses EIGRP can install into the routing table for a prefix. The default is eight paths.
M etr ic Sty le	EIGRP calculates its metric based on bandwidth and delay along with default K values. However, the original 32-bit implementation cannot differentiate interfaces faster than 10 Gigabit Ethernet. This original implementation is called the classic, or narrow, metric. To solve this problem, a 64-bit value with an improved formula was introduced for EIGRP; this is called the wide metric. Valid values for metric style are narrow metric and wide metric. The default is the narrow metric.

Table 9-5 Configuration Parameters in BGP Peer Connectivity Profiles

Configuration Description

nfi
gu
ra
tio
n
Pa
ra
m
et
er

All	Allows ACI to receive routes from eBGP neighbors when the routes have the ACI BGP AS number in the AS_PATH. This option is valid only for eBGP peers.
AS	Allows ACI to overwrite a remote AS in the AS_PATH with the ACI BGP AS. This is typically used when performing Transit Routing from an eBGP L3Out to another eBGP L3Out with the same AS number. Otherwise, an eBGP peer device may not accept the route from ACI because of AS_PATH loop prevention. When this option is enabled, Disable Peer AS Check also needs to be enabled. This option is valid only for eBGP peers.

Dis abl e Pe er AS Ch ec k	Allows ACI to advertise a route to the eBGP peer even if the most recent AS in the <code>AS_PATH</code> of the route is the same as the remote AS for the eBGP peer. This option is valid only for eBGP peers.
Ne xt- ho p Sel f	Allows ACI to update the next-hop address when advertising a route from an eBGP peer to an iBGP peer. By default, route advertisement between iBGP peers keeps the original next-hop address of the route, and the one between eBGP peers always updates the next-hop address with a self IP address.
Se nd Co m m uni ty	When enabled, allows ACI L3Out to advertise routes with a BGP Community attribute, such as <code>AS2:NN</code> format. Otherwise, the BGP Community attribute is stripped when routes are advertised to the outside.

Send Extended Community	<p>When enabled, allows ACI L3Out to advertise routes along with the BGP Extended Community attribute, such as RT:AS2:NN, RT:AS4:NN, and so on. Otherwise, the BGP Extended Community attribute is stripped when routes are advertised to the outside.</p>
Configure Password	<p>When configured, allows the BGP peering to use MD5 authentication on the BGP TCP session. The password can be reset by right-clicking the BGP peer connectivity profile and selecting Reset Password.</p>

All ow ed Sel f AS Co un t	Sets the maximum count for the Allow Self AS option under BGP controls.
Bid ire cti on al For wa rdi ng De tec tio n	Enables BFD on the BGP neighbor.

Dis abl e Co nn ect ed Ch ec k	<p>Provides an alternative to increasing the eBGP multihop TTL in cases where there is a security concern about increasing TTL unnecessarily. For eBGP peering, BGP checks whether the neighbor IP is on the same subnet as any of its local interfaces to see if the neighbor IP is directly connected. If it is not, BGP automatically assumes that the TTL needs to be larger than 1. Hence, when BGP is peering via loopbacks with directly connected routers, the BGP peering is rejected without the eBGP Multihop TTL being set to 2 or larger, even though TTL 1 is technically enough.</p>
Weigh for ro ut es fro m thi s nei ghbo r	<p>Sets the default value of a Cisco proprietary BGP path attribute weight on all the routes learned from the border leaf by the configured peer.</p>

Remove Private AS	<p>In outgoing eBGP route updates to this neighbor, removes all private AS numbers from the AS_PATH when the AS_PATH has only private AS numbers. This option is not applied if the neighbor remote AS is in the AS_PATH.</p>
Remove All Private AS	<p>In outgoing eBGP route updates to this neighbor, removes all private AS numbers from the AS_PATH, regardless of whether a public AS number is included in the AS_PATH. This feature does not apply if the neighbor remote AS is in the AS_PATH. To enable this option, Remove Private AS needs to be enabled.</p>
Replace All Private AS with Local AS	<p>In outgoing eBGP route updates to this neighbor, replaces all private AS numbers in the AS_PATH with ACI local AS, regardless of whether a public AS or the neighbor remote AS is included in the AS_PATH. To enable this option, Remove All Private AS needs to be enabled.</p>

BG P Pe Pre fix Pol icy	Defines an action to take when the number of received prefixes from this neighbor exceeds the configured maximum number. This option is activated by attaching a BGP peer prefix policy to the BGP peer connectivity profile.
Lo cal - AS Nu m be r	Disguises the ACI BGP ASN with the configured local ASN to peer with a particular neighbor. When this feature is used, it looks like there is one more ASN (local AS) between the ACI BGP AS and the external neighbor. Hence, the neighbor peers with the configured local ASN instead of the real ACI BGP ASN. In such situations, both the local ASN and the real ACI BGP ASN are added to the AS_PATH of routes advertised to the neighbor. The local ASN is also prepended to routes learned from the neighbor.

Local ASN number Configuration	<p>Allows granular control over how the local ASN and the fabric ASN appear in the AS_PATHs of routes advertised to external routers or received by the fabric.</p> <p>The no-prepend option prevents ACI from prepending the local ASN in the AS_PATHs of routes learned from this neighbor.</p> <p>The no-prepend, replace-as option allows ACI to add only a local ASN, instead of both a local ASN and a real ACI BGP ASN, to the AS_PATHs of routes advertised to this neighbor on top of the no-prepend option effect.</p> <p>The no-prepend, replace-as, dual-as option allows the neighbor to peer with both a local ASN and a real ACI BGP ASN on top of the no-prepend and replace-as option effect.</p>
Administrative State	Enables a BGP session with a peer to be turned off or on.

Route Control Profile	Allows application of a route profile to a specific BGP neighbor.
-----------------------	---

Table 9-7 Components of a Route Profile

Component	Description
Route Control Profile	The route profile type is specific to ACI. There are two route profile types. One type, Match Prefix AND Routing Policy, combines prefixes from the component that the route profile is associated with and the match criteria configured in the route profile. Components that route profiles can be associated to include bridge domains, bridge domain subnets, L3Outs, L3Out EPGs, and L3Out EPG subnets. The other type, Match Routing Policy Only, only matches routes based on criteria configured in the

route profile and ignores prefixes from the components with which the route profile is associated.

route profile

In a sense, each entry in a route profile includes two context options: Order and Action. Order is equivalent to a sequence number in a normal route map with the caveat that some route profiles merge internal route maps of components with statements explicitly entered by administrators, changing the actual applicable sequence of rules. Action consists of permit or deny and is equivalent in function to permit or deny in a normal route map.

Route profile match rules are similar to match clauses in route maps. Clauses ACI can match against include prefixes, community attributes, and regular expressions.

Route profile match rules

Set rules are equivalent to set clauses in a route map. ACI can set parameters such as community attributes, weight, OSPF types, and AS_PATH.

Set rules

Chapter 10

Table 10-2 Bridge Domain Settings for ACI Layer 2 Extension to Non-ACI Switches

B Required Setting for Property and Justification

D

P
r
o
p
e
r
t
y

Forwarding	<p>The Forwarding field only appears when a bridge domain is first configured. Its default value, Optimized, automatically sets the Unicast and ARP parameters. To enable customization of forwarding settings to values that enable Layer 2 extension, select the Custom option.</p>
L2 Unknown Unicast	<p>This field applies to unicast traffic destined to an endpoint whose MAC address cannot be found in the ACI endpoint table.</p> <p>The forwarding options available for the L2 Unknown Unicast parameter are Flood and Hardware Proxy. When endpoints directly attach to leaf switches and ACI is the default gateway for the BD, hardware proxy forwarding is preferred because it allows for a reduction in flooding within the fabric. However, when some endpoints associated with a bridge domain as well as the default gateway for the BD subnet(s) reside outside the fabric, the ACI spine proxy forwarding behavior can lead to suboptimal learning on non-ACI switches outside the fabric. For this reason, the L2 Unknown Unicast setting needs to be set to Flood to accommodate any endpoints behind the Layer 2 extension until default gateways are moved into the fabric and unicast routing is enabled on the BD.</p>

L By default, IGMP snooping is enabled on bridge domains. **3** The IGMP snooping feature snoops the IGMP membership **U** reports and leave messages and forwards them to the **n** IGMP router function only when necessary. When a leaf **k** receives traffic for a multicast group that is unknown, this **n** traffic is considered unknown Layer 3 multicast, and the **o** L3 Unknown Multicast Flooding setting determines how **w**the traffic is forwarded. The two options for this setting **n** are Flood and Optimized Flood. When Flood is selected, **M**traffic destined to unknown multicast groups is flooded **u**on the ingress switch and any border leafs on which the **I** BD is active. When Optimized Flood is selected, traffic for **t** the unknown multicast group is forwarded to the **i** multicast router ports only.

**c
a
s
t
F
I
o
o
d
i
n
g**

A When the ARP Flooding parameter is enabled, ARP R requests with a broadcast destination MAC address are P flooded in the bridge domain. If this option is disabled F and the fabric has already learned the destination I endpoint, it unicasts the ARP request to the destination. If o this option is disabled and the fabric has *not* learned the

o destination endpoint, it uses ARP gleaning to identify the destination endpoint. When unicast routing is disabled, ARP traffic is always flooded, even if the ARP Flooding parameter has been disabled on the BD.

g

Enabling ARP Flooding ensures that ACI behaves much like traditional networks and allows non-ACI switches behind a Layer 2 extension to proactively learn endpoints residing in the fabric. This, by itself, should be sufficient justification for its use during migrations into ACI. There is one other compelling use case for enabling the ARP Flooding parameter that relates to silent hosts.

Remember from [Chapter 8, “Implementing Tenant Policies,”](#) that ARP gleaning detects silent hosts by prodding them into communicating on the network, but in the rare case that the silent host moves elsewhere without sending a GARP packet into the network, ACI continues to think that the endpoint details it learned prior to the endpoint move are accurate. In this case, if ARP Flooding has been disabled, the ACI leaf continues to unicast ARP requests that are destined to the silent host to the old location until the IP endpoint ages out. On the other hand, with ARP Flooding enabled, ACI floods all ARP requests with broadcast destination MAC addresses.

When the silent host receives the ARP request, it responds to the ARP request, prompting ACI nodes to update the endpoint table accordingly. Even though the issue of silent hosts is not specifically related to Layer 2 extension, this example should help illuminate why the ARP Flooding parameter can help alleviate some corner-case endpoint learning issues.

MThis parameter primarily addresses forwarding of traffic types not covered by the other settings mentioned in this table, such as broadcast, L2 multicast, and link-local traffic. There are three configuration options for the Multi Destination Flooding property:

**D
e
s
t
i
n
a
t
i
o
n
n
a
t
i
o
n
F
I
o
o
d
i
n
g**

Flood in BD: Sends a packet to all ports in the same bridge domain.

Drop: Drops a packet and never sends it to any other ports.

Flood in Encapsulation: Sends a packet to all ports in the same VLAN encapsulation. If there is a one-to-one relationship between encapsulations and EPGs, this setting effectively limits flooding to each EPG.

Note that while Flood in Encapsulation does enable Layer 2 extension and is an option in some deployments, there are more caveats that require careful consideration when using this option for migrations. The Flood in BD option, which is the default setting for the L3 Unknown Multicast

Flooding bridge domain property, remains the most ideal setting for Layer 2 extension.

Table 10-3 Comparison Between Bridge Domain Extension and EPG Extension

Comparison Criteria	Extend EPG	Extend Bridge Domain
Use cases	Extend EPG beyond an ACI fabric; migrate VLANs into ACI in network-centric mode with Flood in BD; consolidate multiple VLANs and subnets into a single bridge domain at the time of migration to ACI by using Flood in Encapsulation	Extend a bridge domain out the fabric or extend a tenant subnet of the bridge domain out the fabric; migrate VLANs into ACI with intra-VLAN policy enforcement applied at the time of migration
Configuration	Statically assign a port to an EPG (static binding under EPG) or direct assignment to an AAEP)	Create external bridged networks (L2Out) in a tenant where a bridge domain resides

Do ma in typ e ap plic abl e	Physical domain	External bridged domain
Ext ern al en dp oin t pla ce me nt	Endpoints connected to non-ACI switches placed in the same EPG (VLAN) as directly attached endpoints	Endpoints connected to non-ACI switches in a different EPG (VLAN) but the same bridge domain as directly attached endpoints
Pol icy mo del	External endpoints are seen as an internal EPG, and the same principles apply.	An external endpoint is placed under an external EPG (Layer 2 EPG). Policy is applied between internal EPGs and a Layer 2 EPG.

En dp oin t lea rni ng	ACI learns both MAC and IP addresses. (IP addresses are only learned if unicast routing is enabled at the BD level.)	ACI learns both MAC and IP addresses. (IP addresses are only learned if unicast routing is enabled at the BD level.)
--	--	--

Chapter 11

Table 11-2 vSphere Teaming and Failover Settings

S	Description
N e t ti n g	<p>N Specifies one of two ways with which a virtual switch can detect network uplink failures. The first, Link Status Only, relies on the operational state of the link. The second option, Beacon Probing, sends probes into the network through its uplinks to see if other uplinks receive the probes. If an uplink is unable to receive the transmitted probes, it is deemed to have suboptimal connectivity.</p> <p>F Use of beacon probing is very uncommon because it requires at least three uplinks to allow the virtual switch to effectively determine which of the uplinks has failed.</p> <p>r The beacon probing option should never be used in combination with port channeling.</p> <p>D</p>

e
t
e
c
t
i
o
n

w i t c h e s	N When set to Yes, prompts the virtual switch repinning a virtual machine to a different uplink following an uplink failure to send a Reverse ARP (RARP) packet into the network in the hope that upstream switches update their CAM tables faster.
F	When all interfaces in the Active Uplinks list have been determined to be non-operational and virtual machines and VMkernel interfaces have been pinned to interfaces in the Standby list, a fallback setting of Yes specifies whether the virtual switch should fall back to interfaces in the Active uplinks list if they become available.
F	Specifies how traffic should be rerouted when an adapter fails. There are three possible adapter states that can be configured in the teaming and failover page: Active Uplinks, Standby Uplinks, and Unused Uplinks. Active uplinks actively forward traffic, while standby uplinks are

only used if all active uplinks fail. An uplink that has been added to the Unused Uplinks list is never used for traffic in a port group, even if both the active and standby uplinks fail.

Chapter 12

Table 12-2 Components of a Device Package

Dev Description	ice Pac kag e Co mp one nt
Dev ice spe cific atio n	An XML file that defines the following: Device properties:

- **Model:** Model of the device
- **Vendor:** Vendor of the device
- **Version:** Software version of the device
- Functions provided by the device
- Interfaces and network connectivity information for each function
- Device configuration parameters
- Configuration parameters for each function

Device script	A Python script that allows the APICs to interact with the device. The device script maps APIC events to function calls. A device package can contain multiple device scripts. A device script can interface with services devices via REST, SSH, or any similar mechanism.
Function profile	An L4-L7 configuration template that includes configuration values for deployment to L4-L7 services devices. When a vendor creates a device package, it typically defines a number of function profiles corresponding with the various functions provided by the services device. The vendor populates default values for a number of parameters within each function profile. Administrators can modify most of the default values to suit their requirements.
Device-level configuration parameters	A configuration file that specifies parameters that are required by a device. This configuration can be shared by one or more service graphs.

Table 12-3 Configuration Options in the Create L4-L7 Devices Page

Configuration Options	
Service Type	<p>Three options are available in this drop-down box:</p> <ul style="list-style-type: none">ADCFirewallOther
Device Type	<p>Possible options available for this parameter include the following:</p>

	<p>Physical: Bare-metal servers, physical appliances, or non-VMM integrated virtual environments</p> <p>Virtual: A VM integrated using a VMM integration</p>
VM Instantiation Policy	This configuration option is part of the service VM orchestration solution and enables APICs to trigger an instantiation of a VM template in vCenter.
Context Aware	<p>This option specifies the context-awareness of the device, which can be one of the following:</p> <p>Single: The device cluster cannot be shared across multiple tenants of a given type that are hosted on the provider network. You must give the device cluster to a specific tenant for a given user.</p>

	<p>Multiple: The device cluster can be shared across multiple tenants of a given type that you are hosting on the provider network. For example, two hosting companies might share the same device.</p>
	<p>When defining a load balancer as a Layer 4 to Layer 7 services device, the Context Aware parameter is not used and can be ignored.</p>
Function Type	This option refers to deployment modes, including GoThrough and GoTo for routed firewalls and transparent firewalls, respectively.

Chapter 15

Table 15-2 Predefined Roles in ACI

Role Name	Description
aaa	Aids in configuring authentication, authorization, accounting, and import/export policies

access-admin	Enables administration and configuration of access policies
admin	
admin	
admin	Provides full access to an ACI fabric
fabric-admin	Enables administration and configuration of fabricwide settings and also firmware management
nw-service-admin	Allows users to configure L4-L7 network service insertion and orchestration
nw-service-params	Grants access to the parameters governing the configuration of external L4-L7 devices
ops	Provides network operator privileges to an ACI fabric to allow for monitoring and troubleshooting functionality in ACI

read-all	Provides read-only visibility into an ACI fabric
tenant-admin-in	When assigned to a limited security domain, allows configuration of most attributes inside a tenant but does not allow changes to fabricwide settings that can potentially impact other tenants
tenant-ext-admin-in	Allows the configuration of external connectivity, such as L3Outs, for ACI tenants; a subset of the tenant-admin role
vm-mgmt-admin-in	Grants access to ACI integrations with virtualization environments such as Microsoft Hyper-V, OpenStack, and VMware vSphere

Table 15-6 Configuration Parameters for LDAP Providers

C Description

o
n
fi
g
ur
at
io
n
P
ar
a
m
et
er

H ACI allows administrators to reference an LDAP server
os by using either its IP address or DNS address.
t
N
a
m
e
or
IP
Ad
dr
es
s

Port	This is the service port number for the LDAP service. The range is from 1 to 65535. The default is 389.
Bind DN	This is a string referencing an account on an LDAP server that is able to query at least a portion of the LDAP directory hierarchy. This account should ideally be a system account with a non-expiring password. In non-production environments leveraging LDAP servers with anonymous bind capabilities, this field can be left empty. LDAP server administrators need to provide ACI administrators the exact Bind DN string.
Base DN	This is a string referencing the container and subtree under which ACI is able to execute queries for matching users using the bind account. LDAP server administrators need to provide ACI administrators the exact Base DN string.
Password	This is the password of the LDAP account specified in the Bind DN field.
Timeout	This is the number of seconds ACI nodes wait for a response from the LDAP provider server. The acceptable range is from 5 to 60 seconds. The default is 30 seconds.

Retries	This is the number of times ACI automatically retries login attempts for a single authentication submission. The acceptable range is from 1 to 5 retries. The default is 1.
Enable SSL	This checkbox allows administrators to enforce SSL-based connections with the LDAP provider.
SSL Certificate Validation Level	Acceptable values for this option are Permissive and Strict. Permissive certificate checking relaxes requirements around certificate validation, making it an ideal option in deployments that use self-signed certificates. Strict certificate validation is ideal in production environments.

Attribute	ACI determines the level of user authorization from the Attribute field. The two most common values for this field are memberOf and CiscoAVPair. When using the memberOf option, configuration of LDAP group map rules is mandatory.
Filter Type	Filters defines how ACI queries an LDAP schema and interprets the existence of a user. The LDAP provider configuration page provides three options for the Filter Type parameter: Default, Microsoft AD, and Custom.
Custom Filter	This is a custom filter value.
Management EPG	This is the management EPG (in-band or out-of-band) from which ACI should source requests to the LDAP server.

Se rv er M on ito rin g	This parameter can be set to either Enabled or Disabled. When it is enabled for an LDAP provider, the APICs periodically attempt to execute login attempts against the LDAP provider to verify that the LDAP service is alive on the server. When enabled, ACI asks administrators to additionally enter a username and password. By default, Server Monitoring is set to Disabled. Server monitoring checks are exclusive to APICs. To enable monitoring checks that leafs and spines are also able to perform, use of the Ping Check option under the AAA Policy view is more common.
--	---

Table 15-7 Settings on the AAA Policy Page

S	Description
et	
ti	
n	
g	

S etting

Re	There are two acceptable values for this setting. Assignm Default Role ensures that any remotely authenticated ot user with a bad or missing Cisco AV pair gets assigned e to the common security domain using the read-all role Us and the privilege type Read. No Login, on the other er hand, ensures that such users cannot log in to the Lo fabric. The default value for this setting is No Login.
Pi	ACI performs ICMP health checks against AAA providers. ng The Ping Check setting can be set to either True or False. C ACI continues to run ICMP health checks against all AAA he providers, regardless of the value chosen. If Ping Check ck is set to True, ACI removes inaccessible providers from the authentication process and authenticates against operational providers instead. If ICMP traffic cannot reach AAA servers due to firewall rules, the Ping Check setting should be set to False to ensure that ACI continues to authenticate against all servers, regardless of the result of ICMP health checks.

S Description et ti n g

D	This setting governs the login domain ACI uses when a user does not select a domain when logging in to the fabric. It also determines the login domain used when a user attempts to log in to the fabric by using the DefaultAuth domain. You can select Local, LDAP, RADIUS, TACACS+, RSA, or SAML for Default Authentication Realm. Local is selected by default. When you select a setting other than Local, an additional Login Domain field appears, allowing selection of the intended domain.
on Re al m	

S etting

Fa ACI comes with a preconfigured login domain called
llb fallback that is set to local authentication by default. The
ac Fallback Check setting, which can be set to True or False,
k enables or disables reliance on the AAA provider ICMP
C health check for activation of the fallback domain. If
he fallback check is set to True and the configured AAA
ck providers respond to ICMP traffic but are unable to
authenticate users, the fallback login domain will be
unavailable, and users may remain locked out of the
fabric. For this reason, Fallback Check is often kept at its
default value of False.

S Description **e**t **t**i **n** **g**

C This parameter allows users to specify the authentication method for console logins to ACI nodes.
on By default, it is set to Local. Other valid options are so LDAP, RADIUS, TACACS+, and RSA. When you select a le setting besides Local, ACI exposes an additional field for A ut you to specify the login domain.

he
nt
ic
ati
on
Re
al
m

Appendix E: Study Planner

Key:

Practice Test
Reading
Review

Element	Task	G o al	F o r m at e	F o r m at e	S e co n d D a t e	C o m p l e t e d (O p t i o n a l)	N o t e s
Introduction	Read Introduction						
1. The Big Picture: Why ACI?	Read Foundation Topics						

1. The Big Picture: Why ACI?	Review Key Topics			
1. The Big Picture: Why ACI?	Define Key Terms			
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 1 in practice test software			
2. Understanding ACI Hardware and Topologies	Read Foundation Topics			
2. Understanding ACI Hardware and Topologies	Review Key Topics			

2. Understand ing ACI Hardware and Topologies	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 2 in practice test software				
3. Initializing an ACI Fabric	Read Foundation Topics				
3. Initializing an ACI Fabric	Review Key Topics				
3. Initializing an ACI Fabric	Review Memory Tables				

3. Initializing an ACI Fabric	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 3 in practice test software				
4. Exploring ACI	Read Foundation Topics				
4. Exploring ACI	Review Key Topics				
4. Exploring ACI	Review Memory Tables				
4. Exploring ACI	Define Key Terms				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 4 in practice test software				
5. Tenant Building Blocks	Read Foundation Topics				
5. Tenant Building Blocks	Review Key Topics				
5. Tenant Building Blocks	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 5 in practice test software				
6. Access Policies	Read Foundation Topics				
6. Access Policies	Review Key Topics				

6. Access Policies	Review Memory Tables			
6. Access Policies	Define Key Terms			
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 6 in practice test software			
7. Implementing Access Policies	Read Foundation Topics			
7. Implementing Access Policies	Review Key Topics			
7. Implementing Access Policies	Define Key Terms			

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 7 in practice test software				
8. Implementing Tenant Policies	Read Foundation Topics				
8. Implementing Tenant Policies	Review Key Topics				
8. Implementing Tenant Policies	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 8 in practice test software				
9. L3Outs	Read Foundation Topics				

9. L3Outs	Review Key Topics				
9. L3Outs	Review Memory Tables				
9. L3Outs	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 9 in practice test software				
10. Extending Layer 2 Outside ACI	Read Foundation Topics				
10. Extending Layer 2 Outside ACI	Review Key Topics				
10. Extending Layer 2 Outside ACI	Review Memory Tables				

10. Extending Layer 2 Outside ACI	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 10 in practice test software				
11. Integrating ACI into vSphere Using VDS	Read Foundation Topics				
11. Integrating ACI into vSphere Using VDS	Review Key Topics				
11. Integrating ACI into vSphere Using VDS	Review Memory Tables				

11. Integrating ACI into vSphere Using VDS	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 11 in practice test software				
12. Implementing Service Graphs	Read Foundation Topics				
12. Implementing Service Graphs	Review Key Topics				
12. Implementing Service Graphs	Review Memory Tables				
	Define Key Terms				

12. Implementing Service Graphs					
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 12 in practice test software				
13. Implementing Management	Read Foundation Topics				
13. Implementing Management	Review Key Topics				
13. Implementing Management	Define Key Terms				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 13 in practice test software				
14. Monitoring ACI Using Syslog and SNMP	Read Foundation Topics				
14. Monitoring ACI Using Syslog and SNMP	Review Key Topics				
14. Monitoring ACI Using Syslog and SNMP	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 14 in practice test software				

15. Implementing AAA and RBAC	Read Foundation Topics				
15. Implementing AAA and RBAC	Review Key Topics				
15. Implementing AAA and RBAC	Define Key Terms				
15. Implementing AAA and RBAC	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 15 in practice test software				
16. ACI Anywhere	Read Foundation Topics				

16. ACI Anywhere	Review Key Topics			
16. ACI Anywhere	Define Key Terms			
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 16 in practice test software			
17. Final Preparation	Read Chapter			
17. Final Preparation	Take practice test in study mode for all Book Questions in practice test software			
17. Final Preparation	Review Exam Essentials for each chapter on the PDF from book page			
17. Final Preparation	Review all Key Topics in all chapters			

17. Final Preparation	Complete all memory tables from the book page			
17. Final Preparation	Take practice test in practice exam mode using Exam Bank #1 questions for all chapters			
17. Final Preparation	Review Exam Essentials for each chapter on the PDF from the book page			
17. Final Preparation	Take practice test in practice exam mode using Exam Bank #2 questions for all chapters			



Where are the companion content files?

Register this digital version of CCNP Data Center Application Centric Infrastructure DCACI 300-620 Official Cert Guide to access important downloads.

Register this eBook to unlock the companion files. Follow these steps:

1. Go to ciscopress.com/account and log in or create a new account.
2. Enter the ISBN: **9780136602668** (NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the “Access Bonus Content” link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit ciscopress.com/practicetest

The Professional and Personal Technology Brands of Pearson



Cisco Press

informIT

PEARSON IT Certification

QUE®

SAMS

CCNP
Data Center
Application Centric
Infrastructure
DCACI 300-620
Official Cert Guide

ISBN: 978-0-13-660266-8

**See other side for your Pearson Test Prep Practice
Test activation code and special offers ►►**

CCNP Data Center
Application Centric
Infrastructure DCACI 300-
620
Official Cert Guide

Premium Edition and Practice Test

To enhance your preparation, Cisco Press also sells a digital Premium Edition of this book. The Premium Edition provides you with three eBook files (PDF, EPUB, and MOBI/Kindle) as well as an enhanced edition of the Pearson IT Certification Practice Test. The Premium Edition includes two additional practice exams with links for every question mapped to the PDF eBook.

Special Offer-Save 80%

This single-use coupon code will allow you to purchase a copy of the Premium Edition at an 80% discount. Simply go to the URL below, add the Premium Edition to your cart, and apply the coupon code at checkout.

www.ciscopress.com/title/9780136588474

Coupon Code:

Complete Video Course

To enhance your preparation, Cisco Press also sells Complete Video Courses for both streaming and download. Complete Video Courses provide you with hours of expert-level instruction mapped directly to exam objectives.

Special Offer-Save 70%

This single-use coupon code will allow you to purchase the Complete Video Course at a **70% discount**. Simply go to the product URL below, add the Complete Video Course to your cart, and apply the coupon code at checkout.

CCNP Data Center Application Centric Infrastructure DCACI 300-620 Complete Video Course

www.ciscopress.com/title/9780136717126

Coupon Code:

DO NOT DISCARD THIS NUMBER

You will need this activation code to activate your practice test in the Pearson Test Prep practice test software. To access the online version, go to www.PearsonTestPrep.com. Select Pearson IT Certification as your product group. Enter your email/password for your account. If you don't have an account

on **PearsonITCertification.com** or **CiscoPress.com**, you will need to establish one by going to www.PearsonITCertification.com/join. In the My Products tab, click the Activate New Product button. Enter the access code printed on this insert card to activate your product. The product will now be listed in your My Products page.

If you wish to use the Windows desktop offline version of the application, simply register your book at www.ciscopress.com/register, select the Registered Products tab on your account page, click the Access Bonus Content link, and download and install the software from the companion website.

This access code can be used to register your exam in both the online and offline versions.

Activation Code:

**CCNP Data Center
Application Centric
Infrastructure
DCACI 300-620
Official Cert Guide**

Enhance Your Exam Preparation

Save 80% on Premium Edition eBook and Practice Test

The *CCNP Data Center Application Centric Infrastructure DCACI 300-620 Official Cert Guide Premium Edition and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.

CCNP Data Center Application Centric Infrastructure DCACI 300-620 Official Cert Guide Companion Website

Access interactive study tools on this book's companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to [**www.ciscopress.com/register**](http://www.ciscopress.com/register).
2. Enter the print book ISBN: **9780136602668..**
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.

6. Under the book listing, click on the **Access Bonus Content** link.

If you have any issues accessing the companion website, you can contact our support team by going to pearsonitp.echelp.org.

Code Snippets

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a “Click here to view code image” link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

```
Cluster configuration ...

Enter the fabric name [ACI Fabric1]: DC1-Fabric1
Enter the fabric ID (1-128) [1]: 1
Enter the number of active controllers in the fabric (1-9) [3]: 3
Enter the POD ID (1-9) [1]: 1
Is this a standby controller? [NO]: NO
Enter the controller ID (1-3) [1]: 1
Enter the controller name [apic1]: DC1-APIC1
Enter address pool for TEP addresses [10.0.0.0/16]: 10.233.44.0/22
Note: The infra VLAN ID should not be used elsewhere in your environment
      and should not overlap with any other reserved VLANs on other platforms.
Enter the VLAN ID for infra network (2-4094): 3600
Enter address pool for BD multicast addresses (GIP0) [225.0.0.0/15]:
```



```
Out-of-band management configuration ...

Enable IPv6 for Out of Band Mgmt Interface? [N] :
Enter the IPv4 address [192.168.10.1/24] : 172.23.142.29/21
Enter the IPv4 address of the default gateway [None] : 172.23.136.1
Enter the interface speed/duplex mode [auto] :

admin user configuration ...

Enable strong passwords? [Y] :
Enter the password for admin:

Reenter the password for admin:

Cluster configuration ...
Fabric name: DC1-Fabric1
Fabric ID: 1
Number of controllers: 3
Controller name: DC1-APIC1
POD ID: 1
Controller ID: 1
TEP address pool: 10.233.44.0/22
Infra VLAN ID: 3600
Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
Management IP address: 172.23.142.29/21
Default gateway: 172.23.136.1
Interface speed/duplex mode: auto

admin user configuration ...

Strong Passwords: Y
User name: admin
Password: *****

The above configuration will be applied ...

Warning: TEP address pool, Infra VLAN ID and Multicast address pool
cannot be changed later, these are permanent until the
fabric is wiped.

Would you like to edit the configuration? (y/n) [n] :
```

```
LEAF101# show isis adjacency detail vrf overlay-1
IS-IS process: isis_infra VRF:overlay-1
IS-IS adjacency database:
System ID          SNPA          Level  State   Hold Time  Interface
212E.E90A.0000    N/A           1       UP      00:01:01  Ethernet1/49.34
Up/Down transitions: 1, Last transition: 21d17h ago
Circuit Type: L1
IPv4 Address: 10.233.46.33
232E.E90A.0000    N/A           1       UP      00:00:55  Ethernet1/50.35
Up/Down transitions: 1, Last transition: 21d17h ago
Circuit Type: L1
IPv4 Address: 10.233.46.35
```

```
LEAF101# show ip int brief | grep -E "lo0|unnumbered"
eth1/49.34          unnumbered           protocol-up/link-up/admin-up
                      (lo0)
eth1/50.35          unnumbered           protocol-up/link-up/admin-up
                      (lo0)
lo0                 10.233.46.32/32    protocol-up/link-up/admin-up
```

```
SPINE201# show ip int brief | grep -E "lo0|unnumbered"
eth1/1.37          unnumbered           protocol-up/link-up/admin-up
                      (lo0)
eth1/2.38          unnumbered           protocol-up/link-up/admin-up
                      (lo0)
lo0                 10.233.46.33/32    protocol-up/link-up/admin-up
```

```
SPINE202# show ip int brief | grep -E "lo0|unnumbered"
eth1/1.35          unnumbered           protocol-up/link-up/admin-up
                      (lo0)
eth1/2.36          unnumbered           protocol-up/link-up/admin-up
                      (lo0)
lo0                 10.233.46.35/32    protocol-up/link-up/admin-up
```

```

LEAF101# show ip int brief vrf overlay-1
(...output truncated for brevity...)
IP Interface Status for VRF "overlay-1"(4)
Interface          Address            Interface Status
eth1/49           unassigned        protocol-up/link-up/admin-up
eth1/49.34         unnumbered       protocol-up/link-up/admin-up
                           (lo0)
eth1/50           unassigned        protocol-up/link-up/admin-up
eth1/50.35         unnumbered       protocol-up/link-up/admin-up
                           (lo0)
vlan8             10.233.44.30/27   protocol-up/link-up/admin-up
lo0               10.233.46.32/32   protocol-up/link-up/admin-up
lo1023            10.233.44.32/32   protocol-up/link-up/admin-up

```

```

LEAF101# show vlan extended

```

VLAN	Name	Encap	Ports
---	---	---	---
8	infra:default	vxlan-16777209, Eth1/1, Eth1/2, Eth1/47	vlan-3600

```
LEAF101# show isis dteps vrf overlay-1
```

IS-IS Dynamic Tunnel End Point (DTEP) database:

DTEP-Address	Role	Encapsulation	Type
10.233.46.33	SPINE	N/A	PHYSICAL
10.233.47.65	SPINE	N/A	PHYSICAL, PROXY-ACAST-MAC
10.233.47.66	SPINE	N/A	PHYSICAL, PROXY-ACAST-V4
10.233.47.64	SPINE	N/A	PHYSICAL, PROXY-ACAST-V6
10.233.46.34	LEAF	N/A	PHYSICAL
10.233.46.35	SPINE	N/A	PHYSICAL

```
LEAF101# show interface tunnel 1-20 | grep -E 'destination|up'

Tunnel1 is up
    Tunnel destination 10.233.46.33

Tunnel3 is up
    Tunnel destination 10.233.46.34

Tunnel4 is up
    Tunnel destination 10.233.46.35

Tunnel5 is up
    Tunnel destination 10.233.47.65

Tunnel6 is up
    Tunnel destination 10.233.47.66

Tunnel7 is up
    Tunnel destination 10.233.47.64

Tunnel8 is up
    Tunnel destination 10.233.44.1

Tunnel9 is up
    Tunnel destination 10.233.44.2

Tunnel10 is up
    Tunnel destination 10.233.44.3
```

```
apic1# cat /etc/ntp.conf

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
tinker panic 501996547

restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.

#restrict default ignore
restrict 127.0.0.1
#restrict -6 ::1

keysdir /etc/ntp/
keys /etc/ntp/keys

server 10.233.48.10 prefer minpoll 4 maxpoll 6
server 10.133.48.10 minpoll 4 maxpoll 6
```

```
apic1# ntpstat
synchronised to NTP server (10.233.48.10) at stratum 4
time correct to within 72 ms
polling server every 16 s
```



```

LEAF101# show ntp peers
-----
--+
Peer IP Address          Serv/Peer Prefer KeyId Vrf
-----+
--+
10.233.48.10           Server    yes     None   management
10.133.48.10           Server    no      None   management

LEAF101# show ntp peer-status
Total peers : 3
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
      remote                  local          st poll reach delay
vrf

-----
--+
*10.233.48.10          0.0.0.0       4  64   3   0.040 management
=10.133.48.10          0.0.0.0       4  64   3   0.040 management

LEAF101# show ntp statistics peer ipaddr 10.233.48.10
remote host:          10.233.48.10
local interface:      Unresolved
time last received:  6s
time until next send: 59s
reachability change: 89s
packets sent:        3
packets received:    3
bad authentication:  0
bogus origin:        0
duplicate:           0
bad dispersion:      0
bad reference time:  0
candidate order:     0

```

```
login as: apic#tacacs_domain\\ammar
Pre-authentication banner message from server:
| Application Policy Infrastructure Controller
End of banner message from server
apic#tacacs-domain\\dcaci@10.100.5.21's password: <Enter Password >
apic1#
```

```
apic1# configure
apic1(config)# dns
apic1(config-dns)# show ?
aaa                  Show AAA information
access-list        Show Access-list Information
(...output truncated for brevity...)
apic1(config-dns)# e?
end                  Exit to the exec mode
exit                 Exit from current mode
export-config      Export Configuration
apic1(config-dns)# show dns <TAB>
dns-address  dns-domain
apic1(config-dns)# show dns-address
Address            Preferred
-----
10.100.1.72        no
10.100.1.71        yes
apic1(config-dns)# no address 10.100.1.72
apic1(config-dns)# end
apic1# configure t
apic1(config)# dns
apic1(config-dns)# exit
apic1(config)#
```

```
apic1# show running-config dns
# Command: show running-config dns
# Time: Mon Oct 28 14:36:08 2019
dns
  address 10.100.1.71 preferred
  domain aci.networksreimagined.com
  use-vrf oob-default
exit
```

```
apic1# bash
admin@apic1:~>
Display all 1898 possibilities? (y or n)
:
          mkmanifest
!
          mknbi-dos
(...output truncated for brevity...)
admin@apic1:~> exit
apic1# bash -c 'uname -ro'
4.14.119atom-3 GNU/Linux
```

```
DC1-LEAF101# show ip route
Incorrect command "show ip route"

DC1-LEAF101# show vrf
  VRF-Name      VRF-I State   Reason
black-hole      3 Up       --
DCACI:Chapter5  6 Up       --
management     2 Up       --
overlay-1       4 Up       --

DC1-LEAF101# show ip route vrf DCACI:Chapter5
IP Route Table for VRF "DCACI: Chapter5"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.233.52.0/24, ubest/mbest: 1/0, attached, direct, pervasive
 *via 10.233.47.66%overlay-1, [1/0], 09w05d, static
10.233.52.1/32, ubest/mbest: 1/0, attached, pervasive
 *via 10.233.52.1, vlan12, [0/0], 09w05d, local, local
```

```
apic1# show run tenant DCACI
# Command: show running-config tenant DCACI
# Time: Sat Sep 21 21:12:14 2019
    tenant DCACI
        vrf context Chapter5
            exit
        bridge-domain BD-CRITICAL-STUFF
            vrf member Chapter5
            exit
        application Critical-Application
            exit
    interface bridge-domain BD-CRITICAL-STUFF
        ip address 10.220.0.1/16 secondary
        exit
    exit
```

```
apic1# show running-config vlan-domain DCACI-Domain
  vlan-domain DCACI-Domain type phys
    vlan-pool DCACI-VLANS
      vlan 910-920
    exit
```

```
apic1# show running-config leaf-interface-profile Leaf101-102-IntProfile
  leaf-interface-profile Leaf101-102-IntProfile
apic1# show running-config leaf-profile Leaf101-102-SwitchProfile
  leaf-profile Leaf101-102-SwitchProfile
    leaf-group Leaf101-Selector
      leaf 101
    leaf-group Leaf102-Selector
      leaf 102
      exit
  leaf-interface-profile Leaf101-102-IntProfile
```

```
LEAF101# show interface ethernet 1/45-46 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth1/45	--	out-of-ser	trunk	full	10G	10Gbase-SR
Eth1/46	--	out-of-ser	trunk	full	10G	10Gbase-SR

```
APIC1# show run
(...output truncated for brevity...)
template policy-group Multiplayer-Gaming-PolGrp
    cdp enable
    vlan-domain member phys type phys
    exit
leaf-interface-profile LEAF101-IntProfile
    leaf-interface-group Multiplayer-Gaming-Servers
        interface ethernet 1/45-46
        policy-group Multiplayer-Gaming-PolGrp
        exit
    exit
```

```
LEAF101# show port-channel summary
Flags: D - Down      P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       S - Suspended   R - Module-removed
       S - Switched    R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
       F - Configuration failed
-----
Group Port-      Type     Protocol Member Ports
      Channel
-----
1    Po1 (SU)      Eth      LACP     Eth1/6 (P)   Eth1/8 (P)
2    Po2 (SU)      Eth      LACP     Eth1/31 (P)  Eth1/32 (P)
```

```

LEAF101# show port-channel summary

Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       S - Suspended      R - Module-removed
       S - Switched       R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
       F - Configuration failed

-----
Group Port-      Type     Protocol   Member Ports
      Channel
-----
1    Po1 (SU)     Eth      LACP       Eth1/6 (P)   Eth1/8 (P)
2    Po2 (SU)     Eth      LACP       Eth1/31 (P)  Eth1/32 (P)  Eth1/35 (D)
                                         Eth1/36 (D)

```

```
template port-channel Multiplayer-Gaming-1-PC-PolGrp
    cdp enable
    vlan-domain member phys type phys
    channel-mode active
    speed 10G
    no negotiate auto
    exit
leaf-interface-profile LEAF101-IntProfile
leaf-interface-group Multiplayer-Server-1
    interface ethernet 1/31
    interface ethernet 1/32
    channel-group Multiplayer-Gaming-1-PC-PolGrp
    exit
exit
```

```
LEAF101# show vpc
```

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id	:	21
Peer status	:	peer adjacency formed ok
vPC keep-alive status	:	Disabled
Configuration consistency status	:	success
Per-vlan consistency status	:	success
Type-2 consistency status	:	success
vPC role	:	primary, operational secondary
Number of vPCs configured	:	1
Peer Gateway	:	Disabled
Dual-active excluded VLANs	:	-
Graceful Consistency Check	:	Enabled
Auto-recovery status	:	Enabled (timeout = 240 seconds)
Operational Layer3 Peer	:	Disabled

vPC Peer-link status

id	Port	Status	Active vlans
--	---	---	---
1		up	-

vPC status

id	Port	Status	Consistency	Reason	Active vlans
--	---	---	---	---	---

```
LEAF101# show vpc
```

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id	:	21
Peer status	:	peer adjacency formed ok
vPC keep-alive status	:	Disabled
Configuration consistency status	:	success
Per-vlan consistency status	:	success
Type-2 consistency status	:	success
vPC role	:	primary, operational secondary
Number of vPCs configured	:	2
Peer Gateway	:	Disabled
Dual-active excluded VLANs	:	-
Graceful Consistency Check	:	Enabled
Auto-recovery status	:	Enabled (timeout = 240 seconds)
Operational Layer3 Peer	:	Disabled

```
vPC Peer-link status
```

id	Port	Status	Active vlans
--	--	--	--
1		up	-

```
vPC status
```

id	Port	Status	Consistency	Reason	Active vlans
--	--	--	--	--	--
685	Po3	up	success	success	-

```
LEAF101# show port-channel summary
```

Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
F - Configuration failed

Group	Port- Channel	Type	Protocol	Member Ports
1	Po1 (SU)	Eth	LACP	Eth1/6 (P) Eth1/8 (P)
2	Po2 (SU)	Eth	LACP	Eth1/31 (P) Eth1/32 (P)
3	Po3 (SU)	Eth	NONE	Eth1/38 (P)

```
template port-channel Multiplayer-Gaming-3-VPC-PolGrp
  cdp enable
  vlan-domain member phys type phys
  speed 10G
  no negotiate auto
  exit
leaf-interface-profile LEAF101-102-vPC-IntProfile
  leaf-interface-group Multiplayer-Server-3
    interface ethernet 1/38
    channel-group Multiplayer-Gaming-3-VPC-PolGrp vpc
    exit
  exit
```

```
APIC1(config)# show running-config all template port-channel
Multiplayer-Gaming-3-VPC-PoGrp
(...output truncated for brevity...)
template port-channel Multiplayer-Gaming-3-VPC-PoGrp
    no description
    lldp receive
    lldp transmit
    cdp enable
    vlan-domain member phys type phys
        channel-mode on
    lacp min-links 1
    lacp max-links 16
    no lacp symmetric-hash
        exit
    mcp enable
    spanning-tree bpdu-filter disable
    spanning-tree bpdu-guard disable
    speed 10G
    no negotiate auto
    exit
```

```
LEAF101# show interface ethernet 1/45-46, ethernet 1/31-32, ethernet 1/38 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth1/31	--	connected	trunk	full	10G	10Gbase-SR
Eth1/32	--	connected	trunk	full	10G	10Gbase-SR
Eth1/38	--	connected	trunk	full	10G	10Gbase-SR
Eth1/45	--	connected	trunk	full	10G	10Gbase-SR
Eth1/46	--	connected	trunk	full	10G	10Gbase-SR

```

LEAF101# show port-channel summary
Flags: D - Down      P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
F - Configuration failed
-----
```

Group	Port- Channel	Type	Protocol	Member Ports	
1	Po1 (SU)	Eth	LACP	Eth1/6 (P)	Eth1/8 (P)
2	Po2 (SU)	Eth	LACP	Eth1/31 (P)	Eth1/32 (P)
3	Po3 (SU)	Eth	NONE	Eth1/38 (P)	
4	Po4 (SU)	Eth	NONE	Eth1/11 (P)	Eth1/12 (P)

FEX	FEX	FEX		
Number	Description	State	Model	Serial
101	FEX0101	Online	N2K-C2248TP-1GE	XXXXX

```
APIC1# show running-config leaf-interface-profile LEAF101-IntProfile
(...output truncated for brevity...)
leaf-interface-profile LEAF101-IntProfile
  leaf-interface-group Port-Channel-to-FEX101
    interface ethernet 1/11-12
    fex associate 101 template FEX101
  exit
exit

APIC1# show running-config fex-profile FEX101
fex-profile FEX101
  fex-interface-group Multiplayer-Gaming-CIMC
    interface ethernet 1/1-24
    policy-group Server-CIMC-PolGrp
  exit
exit
```

```
leaf-interface-profile LEAF103-IntProfile
    leaf-interface-group Breakout-Ports
        interface ethernet 1/1
        interface ethernet 1/5
        interface ethernet 1/6
        breakout 25g-4x
        exit
    leaf-interface-group Multiplayer-Servers-25G
        interface ethernet 1/1/1-4
        interface ethernet 1/5/1-4
        interface ethernet 1/6/1-4
    policy-group Multiplayer-Gaming-PolGrp
    exit
exit
```

```
LEAF101# show copp policy
```

COPP Class	COPP proto	COPP Rate	COPP Burst
lldp	lldp	1000	1000
traceroute	traceroute	500	500
permitlog	permitlog	300	300
nd	nd	1000	1000
icmp	icmp	500	500
isis	isis	1500	5000
eigrp	eigrp	2000	2000
arp	arp	1360	340
cdp	cdp	1000	1000
ifcspan	ifcspan	2000	2000
ospf	ospf	2000	2000
bgp	bgp	5000	5000
tor-glean	tor-glean	100	100
acllog	acllog	500	500

mcp	mcp	1500	1500
pim	pim	500	500
igmp	igmp	1500	1500
ifc	ifc	7000	7000
coop	coop	5000	5000
dhcp	dhcp	1360	340
ifcother	ifcother	332800	5000
infraarp	infraarp	300	300
lacp	lacp	1000	1000
glean	glean	100	100
stp	stp	1000	1000

```
LEAF101# show copp policy
```

COPP Class	COPP proto	COPP Rate	COPP Burst
lldp	lldp	10	10
traceroute	traceroute	10	10
permitlog	permitlog	10	10
nd	nd	10	10
icmp	icmp	10	10
isis	isis	10	10
eigrp	eigrp	10	10
arp	arp	10	10
cdp	cdp	10	10
ifcspan	ifcspan	10	10
ospf	ospf	10	10
bgp	bgp	10	10
tor-glean	tor-glean	10	10
acllog	acllog	10	10
mcp	mcp	10	10
pim	pim	10	10
igmp	igmp	10	10
ifc	ifc	7000	7000
coop	coop	10	10
dhcp	dhcp	10	10
ifcother	ifcother	10	10
infraarp	infraarp	10	10
lacp	lacp	10	10
glean	glean	10	10
stp	stp	10	10

```
LEAF101# show port-channel summary interface port-channel 2
```

```
Flags: D - Down P - Up in port-channel (members)
```

```
I - Individual H - Hot-standby (LACP only)
```

```
s - Suspended r - Module-removed
```

```
S - Switched R - Routed
```

```
U - Up (port-channel)
```

```
M - Not in use. Min-links not met
```

```
F - Configuration failed
```

Group	Port- Channel	Type	Protocol	Member Ports
-------	------------------	------	----------	--------------

2	Po2(SD)	Eth	LACP	Eth1/31(P) Eth1/32(P)
---	---------	-----	------	-----------------------

```
LEAF101# show lacp interface ethernet 1/31 | egrep -A8 "Local" | egrep "Local|LACP"
```

```
Local Port: Eth1/31 MAC Address= 00-27-e3-15-bd-e3
```

```
    LACP _ Activity=active
```

```
    LACP _ Timeout=Long Timeout (30s)
```

```
LEAF101# show lacp interface ethernet 1/32 | egrep -A8 "Local" | egrep "Local|LACP"
```

```
Local Port: Eth1/32 MAC Address= 00-27-e3-15-bd-e3
```

```
    LACP _ Activity=active
```

```
    LACP _ Timeout=Long Timeout (30s)
```

```
LEAF101# show lacp interface ethernet 1/31 | egrep -A8 "Local" | egrep "Local|LACP"
Local Port: Eth1/31    MAC Address= 00-27-e3-15-bd-e3
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
LEAF101# show lacp interface ethernet 1/32 | egrep -A8 "Local" | egrep "Local|LACP"
Local Port: Eth1/32    MAC Address= 00-27-e3-15-bd-e3
  LACP_Activity=active
  LACP_Timeout=Short Timeout (1s)
```

```
LEAF102# show vlan id 30,31 extended
```

VLAN	Name	Encap	Ports
30	Production:Multiplayer-Servers-BD	vxlan-16613250	Eth1/38, Po2
31	Production:3rd-Party:Servers-EPG	vlan-302	Eth1/38, Po2

```
LEAF102# show vrf Production:MP detail extended | grep vxlan
```

```
Encap: vxlan-2981888
```

```
LEAF102# show endpoint ip 10.233.58.20
```

Legend:

s - arp	H - vtep	V - vpc-attached	p - peer-aged
R - peer-attached-rl	B - bounce	S - static	M - span
D - bounce-to-proxy	O - peer-attached	a - local-aged	m - svc-mgr
L - local		E - shared-service	
-----+-----+-----+-----+			
VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info
-----+-----+-----+-----+			

76	vlan-3171	0050.56b7.c60a	L	eth1/46
Prod:Temp	vlan-3171	10.233.58.20	L	eth1/46

```
LEAF102# show endpoint ip 10.233.58.32
```

Legend:

s - arp	H - vtep	V - vpc-attached	p - peer-aged
R - peer-attached-rl	B - bounce	S - static	M - span
D - bounce-to-proxy	O - peer-attached	a - local-aged	m - svc-mgr
L - local		E - shared-service	
-----+-----+-----+-----+			
VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info
-----+-----+-----+-----+			

73	vlan-3169	0050.56b7.751d	L	eth1/45
Prod:Temp	vlan-3169	10.233.58.32	L	eth1/45

```
LEAF101# show ip int brief vrf Prod:Temp
IP Interface Status for VRF " Prod:Temp"(23)
Interface          Address           Interface Status
vlan72            10.233.58.1/24    protocol-up/link-up/admin-up

LEAF101# show ip route 10.233.58.1 vrf Prod:Temp
10.233.58.1/32, ubest/mbest: 1/0, attached, pervasive
*via 10.233.58.1, vlan72, [0/0], 05w01d, local, local

LEAF102# show ip int brief vrf Prod:Temp
IP Interface Status for VRF "Prod:Temp"(25)
Interface          Address           Interface Status
vlan65            10.233.58.1/24    protocol-up/link-up/admin-up

LEAF102# show ip route 10.233.58.1 vrf Prod:Temp
10.233.58.1/32, ubest/mbest: 1/0, attached, pervasive
*via 10.233.58.1, vlan65, [0/0], 05w01d, local, local
```

```
LEAF101# show vlan id 72 extended
```

VLAN	Name	Encap	Ports
<hr/>			
72	Prod:BD-Temp	vxlan-15826916	Eth1/45, Eth1/46

```
LEAF102# show vlan id 65 extended
```

VLAN	Name	Encap	Ports
<hr/>			
65	Prod:BD-Temp	vxlan-15826916	Eth1/45, Eth1/46

```
LEAF102# show endpoint ip 10.233.59.50
```

Legend:

s - arp	H - vtep	V - vpc-attached	p - peer-aged
R - peer-attached-rl	B - bounce	S - static	M - span
D - bounce-to-proxy	O - peer-attached	a - local-aged	m - svc-mgr
L - local		E - shared-service	

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface
66	vlan-3172	0050.56b7.a88b	0	tunnel2
Prod:Temp	vlan-3172	10.233.59.50	0	tunnel2

```
LEAF102# show interface tunnel 2
```

Tunnel2 is up

MTU 9000 bytes, BW 0 Kbit

Transport protocol is in VRF "overlay-1"

Tunnel protocol/transport is ivxlan

Tunnel source 10.233.60.226/32 (lo0)

Tunnel destination 10.233.60.224

Last clearing of "show interface" counters never

Tx

0 packets output, 1 minute output rate 0 packets/sec

Rx

0 packets input, 1 minute input rate 0 packets/sec

APIC1# acidiag fnvread

```
LEAF102# show system internal epm endpoint ip 10.233.59.50

MAC : 0000.0000.0000 :: Num IPs : 1
IP# 0 : 10.233.59.50 :: IP# 0 flags : :: l3-sw-hit: No
Vlan id : 0 :: Vlan vniid : 0 :: VRF name : Prod:Temp
BD vniid : 0 :: VRF vniid : 2228225
Phy If : 0 :: Tunnel If : 0x18010002
Interface : Tunnel2
Flags : 0x80004400 :: sclass : 49161 :: Ref count : 3
EP Create Timestamp : 06/02/2020 06:07:58.418861
EP Update Timestamp : 06/02/2020 06:07:58.418861
EP Flags : IP|sclass|timer|
```

```
LEAF101# show system internal epm vpc
(...output truncated for brevity...)
Local TEP IP : 10.233.60.224
Peer TEP IP : 10.233.60.226
vPC configured : Yes
vPC VIP : 10.233.62.131
MCT link status : Up
Local vPC version bitmap : 0x7
Peer vPC version bitmap : 0x7
Negotiated vPC version : 3
Peer advertisement received : Yes
Tunnel to vPC peer : Up
```

```
LEAF102# show endpoint ip 10.233.59.100
```

Legend:

s - arp	H - vtep	V - vpc-attached	p - peer-aged
R - peer-attached-rl	B - bounce	S - static	M - span
D - bounce-to-proxy	O - peer-attached	a - local-aged	m - svc-mgr
L - local	E - shared-service		

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface

```
LEAF102# show ip route 10.233.59.100 vrf Prod:Temp
IP Route Table for VRF "Prod:Temp"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.233.59.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.233.62.130%overlay-1, [1/0], 06:50:59, static, tag 4294967294
    recursive next hop: 10.233.62.130/32%overlay-1
```

```
LEAF102# show isis dteps vrf overlay-1
IS-IS Dynamic Tunnel End Point (DTEP) database:
DTEP-Address      Role    Encapsulation   Type
10.233.60.224    LEAF    N/A              PHYSICAL
10.233.60.225    SPINE   N/A              PHYSICAL
10.233.62.130    SPINE   N/A              PHYSICAL, PROXY-ACAST-V4
10.233.62.129    SPINE   N/A              PHYSICAL, PROXY-ACAST-MAC
10.233.62.128    SPINE   N/A              PHYSICAL, PROXY-ACAST-V6
10.233.60.227    SPINE   N/A              PHYSICAL
10.233.62.131    LEAF    N/A              PHYSICAL
```

```
LEAF101# show vlan extended
(...output truncated for brevity...)
VLAN Name                                Encap        Ports
-----  -----
69      Gaming-BU:BD-Production           vxlan-16285613  Eth1/38, Po3
70      Gaming-BU:Multiplayer-App1:EPG-Client-VMs  vlan-271   Eth1/38, Po3
```

```
LEAF101# show ip int brief vrf Gaming-BU:Multiplayer-Prod
IP Interface Status for VRF "Gaming-BU:Multiplayer-Prod" (23)
Interface          Address            Interface Status
vlan69            10.233.58.1/24      protocol-up/link-up/admin-up

LEAF101# show ip route vrf Gaming-BU:Multiplayer-Prod
IP Route Table for VRF "Gaming-BU:Multiplayer-Prod"
'**' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.233.58.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.233.62.130%overlay-1, [1/0], 09:16:13, static, tag 4294967294
10.233.58.1/32, ubest/mbest: 1/0, attached, pervasive
  *via 10.233.58.1, vlan69, [0/0], 09:16:13, local, local
```

```
LEAF101# show zoning-rule contract Players-to-Login-Servers
```

SrcEPG	DstEPG	Dir	operSt	Scope	Name	Action
16389	32780	uni-dir	enabled	2228225	Players-to-Login-Servers	permit
32780	16389	uni-dir	enabled	2228225	Players-to-Login-Servers	permit

```

LEAF101# show bgp sessions vrf overlay-1
Total peers 5, established peers 5
ASN 65000
VRF overlay-1, local ASN 65000
peers 2, established peers 2, local router-id 10.233.46.32
State: I-Idle, A-Active, O-Open, E-Established, C-Closing, S-Shutdown

Neighbor      ASN   Flaps LastUpDn|LastRead|LastWrit St Port(L/R)  Notif(S/R)
10.233.46.33  65000 0     16w06d |never    |never    E  60631/179  0/0
10.233.46.35  65000 0     16w06d |never    |never    E  44567/179  0/0
LEAF101# acidiag fnvread | grep spine
  201      1      SPINE201      FDOXXXX1      10.233.46.33/32  spine  active  0
  202      1      SPINE202      FDOXXXX2      10.233.46.35/32  spine  active  0

```

```
LEAF301# show ip eigrp neighbors vrf Gaming-BU:Multiplayer-Prod
EIGRP neighbors for process 100 VRF Gaming-BU:Multiplayer-Prod
      H   Address          Interface      Hold   Uptime    SRTT     RTO   Q   Seq
                                         (sec)           (ms)
      0   10.233.75.161      eth1/9        13    07:30:37  1      50   0   19
```

```
LEAF301# show ip route vrf Gaming-BU:Multiplayer-Prod
IP Route Table for VRF "Gaming-BU:Multiplayer-Prod"
(...output truncated for brevity...)
10.199.90.0/24, ubest/mbest: 1/0
    *via 10.233.75.161, eth1/9, [90/128576], 22:35:22, eigrp-default, internal
10.200.1.0/24, ubest/mbest: 1/0
    *via 10.233.75.161, eth1/9, [90/128576], 22:43:09, eigrp-default, internal
10.200.100.0/24, ubest/mbest: 1/0
    *via 10.233.75.161, eth1/9, [90/128576], 23:01:31, eigrp-default, internal

LEAF302# show ip route vrf Gaming-BU:Multiplayer-Prod
IP Route Table for VRF "Gaming-BU:Multiplayer-Prod"
(...output truncated for brevity...)
10.199.90.0/24, ubest/mbest: 1/0
    *via 10.233.60.234%overlay-1, [200/128576], 22:43:13, bgp-65000, internal, tag 65000
10.200.1.0/24, ubest/mbest: 1/0
    *via 10.233.60.234%overlay-1, [200/128576], 22:51:01, bgp-65000, internal, tag 65000
10.200.100.0/24, ubest/mbest: 1/0
    *via 10.233.60.234%overlay-1, [200/128576], 23:09:23, bgp-65000, internal, tag 65000
```

```
LEAF301# show ip arp vrf Gaming-BU:Multiplayer-Prod
```

Flags: * - Adjacencies learnt on non-active FHRP router
+ - Adjacencies synced via CFSoE
- Adjacencies Throttled for Glean
D - Static Adjacencies attached to down interface

IP ARP Table for context Gaming-BU:Multiplayer-Prod

Total number of entries: 1

Address	Age	MAC Address	Interface
10.233.75.161	00:02:30	a0e0.af66.c5a1	eth1/9

```
LEAF301# show ip route ospf vrf Gaming-BU:Multiplayer-Prod
IP Route Table for VRF "Gaming-BU:Multiplayer-Prod"
*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
*via 10.198.10.2, vlan76, [110/5], 00:01:02, ospf-default, inter
```

```
LEAF301# show track
```

Track 2

IP SLA 2256

reachability is down

1 changes, last change 2020-07-11T19:23:25.179+00:00

Tracked by:

Track List 1

Track 3

IP SLA 2288

reachability is up

2 changes, last change 2020-07-11T19:23:25.181+00:00

Tracked by:

Track List 1

Track 1

List Threshold percentage

Threshold percentage is down

1 changes, last change 2020-07-11T19:23:25.176+00:00

Threshold percentage up 51% down 50%

Tracked List Members:

Object 3 (50)% up

Object 2 (50)% down

Attached to:

Route prefix 0.0.0.0/0

```
Router# show ip bgp 10.233.58.0/24 vrf LAB-BGP
(...output truncated for brevity...)
BGP routing table information for VRF LAB-BGP, address family IPv4 Unicast
BGP routing table entry for 10.233.58.0/24, version 14
Paths: (1 available, best #1)
AS-Path: 65000 , path sourced external to AS
    10.197.1.1 (metric 0) from 10.197.1.1 (10.233.75.170)
        Origin incomplete, MED 0, localpref 100, weight 0
    Community: 65000:100
```

Path-id 1 not advertised to any peer

```
LEAF102# show vlan extended
```

VLAN	Name	Encap	Ports
27	Gaming-BU:Multiplayer-App1:EPG-VLAN272	vlan-272	Eth1/6, Po5
28	Gaming-BU:Multiplayer-App1:EPG-Client-VMs	vlan-272	Eth1/33
54	Gaming-BU:BD-VLAN272	vxlan-15040469	Eth1/6, Eth1/45, Eth1/46, Po5
61	Gaming-BU:Multiplayer-App1:EPG-VLAN272	vlan-2508	Eth1/45, Eth1/46
65	Gaming-BU:BD-Production	vxlan-15826916	Eth1/33, Eth1/45, Eth1/46
73	Gaming-BU:Multiplayer-App1:EPG-Client-VMs	vlan-3169	Eth1/45, Eth1/46

```
interface GigabitEthernet0/0
    nameif externalIf
    security-level 50
    ip address 10.91.1.1 255.255.255.0
!
interface GigabitEthernet0/1
    nameif internalIf
    security-level 100
    ip address 10.92.1.1 255.255.255.0
!
object network web_server
    subnet 10.92.1.0 255.255.255.0
access-list access-list-inbound extended permit tcp any object web_server eq www
access-list access-list-inbound extended permit tcp any object web_server eq https
access-group access-list-inbound in interface externalIf
```

```
APIC1# ping 10.233.65.81 -c 2
PING 10.233.65.81 (10.233.65.81) 56(84) bytes of data.
64 bytes from 10.233.65.81: icmp_seq=1 ttl=64 time=0.140 ms
64 bytes from 10.233.65.81: icmp_seq=2 ttl=64 time=0.152 ms

--- 10.233.65.81 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.140/0.155/0.173/0.013 ms
```

```
APIC1# bash
admin@APIC1:~> route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref Use Iface
0.0.0.0         10.234.10.1   0.0.0.0        UG    16    0    0 oobmgmt
0.0.0.0         10.233.65.81  0.0.0.0        UG    32    0    0 bond0.266
10.233.60.0    10.233.60.30  255.255.252.0  UG    0     0    0 bond0.260
10.233.60.30  0.0.0.0       255.255.255.255 UH    0     0    0 bond0.260
10.233.65.80  0.0.0.0       255.255.255.240 U      0     0    0 bond0.266
10.233.65.81  0.0.0.0       255.255.255.255 UH    0     0    0 bond0.266
10.234.10.0    0.0.0.0       255.255.254.0  U      0     0    0 oobmgmt
169.254.1.0    0.0.0.0       255.255.255.0  U      0     0    0 teplo-1
169.254.254.0 0.0.0.0       255.255.255.0  U      0     0    0 lxcbr0
172.17.0.0     0.0.0.0       255.255.0.0   U      0     0    0 docker0
```

```
admin@APIC1:~> route -n
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.233.65.81	0.0.0.0	UG	8	0	0	bond0.266
0.0.0.0	10.234.10.1	0.0.0.0	UG	16	0	0	oobmgmt
10.233.60.0	10.233.60.30	255.255.252.0	UG	0	0	0	bond0.260
10.233.60.30	0.0.0.0	255.255.255.255	UH	0	0	0	bond0.260
10.233.65.80	0.0.0.0	255.255.255.240	U	0	0	0	bond0.266
10.233.65.81	0.0.0.0	255.255.255.255	UH	0	0	0	bond0.266
10.234.10.0	0.0.0.0	255.255.254.0	U	0	0	0	oobmgmt
169.254.1.0	0.0.0.0	255.255.255.0	U	0	0	0	teplo-1
169.254.254.0	0.0.0.0	255.255.255.0	U	0	0	0	lxcbr0
172.17.0.0	0.0.0.0	255.255.0.0	U	0	0	0	docker0

timestamp Nexus: FACILITY-SEVERITY-MNEMONIC: Message-text

2014 Jan 25 21:42:07 Nexus: ETHPORT-5-IF_DOWN_ADMIN_DOWN:
Interface Ethernet3/1 is down (Administratively down)

```
timestamp host %LOG_LOCALn-severity-SYSTEM_MSG [code] [lifecycle  
state] [rule] [severity text] [DN of affected MO]
```

Message-text

July 22 22:45:28 apic1 %LOG_LOCAL0-2-SYSTEM_MSG [F0110] [soaking] [node-failed]
[critical] [topology/pod-1/node-102/fault-F0110]

Node 102 not reachable. unknown

July 22 22:45:27 apic1 *LOG_LOCAL0-6-SYSTEM_MSG [E4208219] [link-state-change] [info]
[subj-[topology/pod-1/lnkcnt-1/lnk-101-1-1-to-1-1-3]/rec-4294968577]
Link State of Fabric Link is set to ok

```
apic1# logit severity 1 dest-grp Syslog-Servers server 10.233.48.10 "This is a test"
      node 101

apic1# logit severity 1 dest-grp Syslog-Servers server 10.233.48.10 "This is a test"
      node 102

apic1# logit severity 1 dest-grp Syslog-Servers server 10.133.48.10 "This is a test"
      node 101

apic1# logit severity 1 dest-grp Syslog-Servers server 10.133.48.10 "This is a test"
      node 102
```

```
apic1# moquery -c syslogSrc -x 'rsp-subtree=children' | grep -E "name  
|dn|incl|monPolDn|tDn|^$"  
  
name      : common-syslog  
dn        : uni/fabric/moncommon/slsrc-common-syslog  
incl      : all,audit,events,faults,session  
monPolDn  : uni/fabric/moncommon  
  
dn        : uni/fabric/moncommon/slsrc-common-syslog/rsdestGroup  
monPolDn  : uni/fabric/moncommon  
tDn      : uni/fabric/slgroup-Syslog-Servers  
  
name      : fabric-syslog  
dn        : uni/fabric/monfab-default/slsrc-fabric-syslog
```

```
incl      : all,audit,events,faults,session
monPolDn  : uni/fabric/monfab-default

dn        : uni/fabric/monfab-default/slsrc-fabric-syslog/rsdestGroup
monPolDn  : uni/fabric/monfab-default
tDn       : uni/fabric/slgroup-Syslog-Servers

name      : access-syslog
dn        : uni/infra/moninfra-default/slsrc-access-syslog
incl      : all,audit,events,faults,session
monPolDn  : uni/infra/moninfra-default

dn        : uni/infra/moninfra-default/slsrc-access-syslog/rsdestGroup
monPolDn  : uni/infra/moninfra-default
tDn       : uni/fabric/slgroup-Syslog-Servers

name      : tenant-syslog
dn        : uni/tn-common/monepg-default/slsrc-tenant-syslog
incl      : all,audit,events,faults,session
monPolDn  : uni/tn-common/monepg-default

dn        : uni/tn-common/monepg-default/slsrc-tenant-syslog/rsdestGroup
monPolDn  : uni/tn-common/monepg-default
tDn       : uni/fabric/slgroup-Syslog-Servers
```

```
apic1# moquery -c syslogRemoteDest | grep -E '#|host|adminState|epgDn|severity'  
# syslog.RemoteDest  
host : 10.133.48.10  
adminState : enabled  
epgDn : uni/tn-mgmt/mgmtp-default/oob-default  
severity : warnings  
# syslog.RemoteDest  
host : 10.233.48.10  
adminState : enabled  
epgDn : uni/tn-mgmt/mgmtp-default/oob-default  
severity : warnings
```

```
apic1# show snmp
(...output truncated for brevity...)
Input Statistics:
    34 SNMP packets input
    0 Trap PDUs received
    48 Get-next PDUs
    0 General Errors
    0 Set-request PDUs
    44 Number of requested variables
Output Statistics:
    0 Get-request PDUs generated
    58 Get-responses PDUs generated
    0 Set-requests PDUs generated
    34 SNMP packets output
Other Statistics:
    0 Silent Drops
    0 Proxy Drops
Disabled Authentication Traps Status
Name          Admin State  Location      Contact           Description
-----
default       enabled            Ammar Ahmadi
```

```
apic1# show snmp summary
```

```
Active Policy: default, Admin State: enabled
```

```
Local SNMP engineID: [Hex] 0x800000098057dbed2fc3d3c45d00000000
```

```
-----  
Community Description
```

```
HelloWorld Global scope string  
DCACI-context-password DCACI-VRF-Specific
```

```
-----  
User Authentication Privacy
```

```
-----  
Client-Group Mgmt-Epg Clients
```

```
-----  
SNMP-Servers default (Out-Of-Band) 10.133.48.10,10.233.48.10
```

```
-----  
Host Port Version Level SecName
```

```
-----  
10.233.48.10 162 v2c noauth HelloWorld  
10.133.48.10 162 v2c noauth HelloWorld
```

```
apic1# moquery -c snmpSrc -x 'rsp-subtree=children'
Total Objects shown: 1
(...output truncated for brevity...)
# snmp.Src
name      : common-snmp
dn        : uni/fabric/moncommon/snmpsrc-common-snmp
incl      : events,faults
```

```
monPolDn      : uni/fabric/moncommon
rn            : snmpsrc-common-snmp

# snmp.RsDestGroup
dn            : uni/fabric/moncommon/snmpsrc-common-snmp/rsdestGroup
monPolDn      : uni/fabric/moncommon
tDn          : uni/fabric/snmpgroup-SNMP-Monitoring-Servers
```

```
APIC1(config)# show run
(...output truncated for brevity...)
tacacs-server host "10.233.48.60"
exit
tacacs-server host "10.233.64.60"
exit
aaa group server tacacsplus TACACS
  server 10.233.48.60 priority 1
  server 10.233.64.60 priority 2
exit
aaa authentication login domain TACACS
  realm tacacs
  group TACACS
exit
```

```
shell:domains = domainA/writeRole1|writeRole2|writeRole3/  
readRole1|readRole2,  
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2
```

```
shell:domains = domainA/writeRole1|writeRole2|writeRole3/  
readRole1|readRole2,  
domainB/writeRole1|writeRole2|writeRole3/  
readRole1|readRole2(userId)
```

```
APIC1(config)# show run
(...output truncated for brevity...)
radius-server host "10.233.48.67"
exit
aaa group server radius RADIUS
  server 10.233.48.67 priority 1
  exit
aaa authentication login domain RADIUS
  realm radius
  group RADIUS
  exit
```

Contents

[Cover Page](#)

[About This eBook](#)

[Title Page](#)

[Copyright Page](#)

[About the Author](#)

[About the Technical Reviewers](#)

[Dedication](#)

[Acknowledgments](#)

[Contents at a Glance](#)

[Reader Services](#)

[1. Other Features](#)

[Contents](#)

[Icons Used in This Book](#)

[Command Syntax Conventions](#)

[Introduction](#)

[1. Perspectives on the DCACI 300-620 Exam](#)

[2. Who Should Read This Book?](#)

3. The Companion Website for Online Content Review
4. How to Access the Pearson Test Prep (PTP) App
5. How This Book Is Organized
6. How to Use This Book

Figure Credit

Part I Introduction to Deployment

1. Chapter 1 The Big Picture: Why ACI?
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. Understanding the Shortcomings of Traditional Networks
 1. Network Management
 2. Scalability and Growth
 3. Network Agility
 4. Security
 5. Network Visibility
 4. Recognizing the Benefits of Cisco ACI
 1. Network Management Touchpoints
 2. Traffic Flow Optimizations
 3. Scalability Optimizations

4. Programmability
 5. Stateless Network
 6. Multitenancy
 7. Zero-Trust Security
 8. Cross-Platform Integrations
 9. New Architectural Possibilities
 10. Integrated Health Monitoring and Enhanced Visibility
 11. Policy Reuse
5. Exam Preparation Tasks
 6. Review All Key Topics
 7. Complete Tables and Lists from Memory
 8. Define Key Terms
2. Chapter 2 Understanding ACI Hardware and Topologies
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. ACI Topologies and Components
 1. Clos Topology
 2. Standard ACI Topology
 3. ACI Stretched Fabric Topology

- 4. ACI Multi-Pod Topology
 - 5. ACI Multi-Site Topology
 - 6. ACI Multi-Tier Architecture
 - 7. Remote Leaf Topology
4. APIC Clusters
- 1. APIC Cluster Scalability and Sizing
5. Spine Hardware
- 1. First-Generation Spine Switches
 - 2. Second-Generation Spine Switches
6. Leaf Hardware
- 1. First-Generation Leaf Switches
 - 2. Second-Generation Leaf Switches
7. Exam Preparation Tasks
8. Review All Key Topics
9. Complete Tables and Lists from Memory
10. Define Key Terms
3. Chapter 3 Initializing an ACI Fabric
- 1. “Do I Know This Already?” Quiz
 - 2. Foundation Topics
 - 3. Understanding ACI Fabric Initialization

1. Planning Fabric Initialization
 2. Understanding Cabling Requirements
 3. Connecting APICs to the Fabric
 4. Initial Configuration of APICs
 5. APIC OOB Configuration Requirements
 6. Out-of-Band Versus In-Band Management
 7. Configuration Information for Fabric Initialization
 8. Switch Discovery Process
 9. Fabric Discovery Stages
 10. Switch Discovery States
4. Initializing an ACI Fabric
 1. Changing the APIC BIOS Password
 2. Configuring the APIC Cisco IMC
 3. Initializing the First APIC
 4. Discovering and Activating Switches
 5. Understanding Graceful Insertion and Removal (GIR)
 6. Initializing Subsequent APICs
 7. Understanding Connectivity Following Switch Initialization

5. Basic Post-Initialization Tasks

1. Assigning Static Out-of-Band Addresses to Switches and APICs
2. Applying a Default Contract to Out-of-Band Subnet
3. Upgrading an ACI Fabric
4. Understanding Schedulers
5. Enabling Automatic Upgrades of New Switches
6. Understanding Backups and Restores in ACI
7. Making On-Demand Backups in ACI
8. Making Scheduled Backups in ACI
9. Taking Configuration Snapshots in ACI
10. Importing Configuration Backups from Remote Servers
11. Executing Configuration Rollbacks
12. Pod Policy Basics
13. Configuring Network Time Protocol (NTP) Synchronization
14. Configuring DNS Servers for Lookups
15. Verifying COOP Group Configurations

6. Exam Preparation Tasks
 7. Review All Key Topics
 8. Complete Tables and Lists from Memory
 9. Define Key Terms
4. Chapter 4 Exploring ACI
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. ACI Access Methods
 1. GUI
 2. CLI
 3. APIC CLI
 4. Switch CLI
 5. API
 6. Management Access Modifications
4. Understanding the ACI Object Model
 1. Learning ACI Through the Graphical User Interface
 2. Exploring the Object Hierarchy by Using Visore
 3. Why Understand Object Hierarchy Basics for DCACI?

4. Policy in Context
5. Integrated Health Monitoring and Enhanced Visibility
 1. Understanding Faults
 2. The Life of a Fault
 3. Acknowledging Faults
 4. Faults in the Object Model
 5. Monitoring Policies in ACI
 6. Customizing Fault Management Policies
 7. Squelching Faults and Changing Fault Severity
 8. Understanding Health Scores
 9. Understanding Events
 10. Squelching Events
 11. Understanding Audit Logs
6. Exam Preparation Tasks
 7. Review All Key Topics
 8. Complete Tables and Lists from Memory
 9. Define Key Terms

Part II ACI Fundamentals

1. Chapter 5 Tenant Building Blocks

1. “Do I Know This Already?” Quiz
2. Foundation Topics
3. Understanding the Basic Objects in Tenants
 1. Tenants
 2. Predefined Tenants in ACI
 3. VRF Instances
 4. Bridge Domains (BDs)
 5. Endpoint Groups (EPGs)
 6. Application Profiles
 7. The Pain of Designing Around Subnet Boundaries
 8. BDs and EPGs in Practice
 9. Configuring Bridge Domains, Application Profiles, and EPGs
 10. Classifying Endpoints into EPGs
 11. APIC CLI Configuration of Tenant Objects
4. Contract Security Enforcement Basics
 1. Contracts, Subjects, and Filters
 2. Contract Direction
 3. Contract Scope
 4. Zero-Trust Using EPGs and Contracts

5. Objects Enabling Connectivity Outside the Fabric

1. External EPGs
2. Layer 3 Outside (L3Out)

6. Tenant Hierarchy Review

7. Exam Preparation Tasks
8. Review All Key Topics

9. Complete Tables and Lists from Memory

10. Define Key Terms

2. Chapter 6 Access Policies

1. “Do I Know This Already?” Quiz
2. Foundation Topics
3. Pools, Domains, and AAEPs
 1. VLAN Pools
 2. Domains
 3. Common Designs for VLAN Pools and Domains
 4. Challenges with Overlap Between VLAN Pools
 5. Attachable Access Entity Profiles (AAEPs)
4. Policies and Policy Groups

1. Interface Policies and Interface Policy Groups
 2. Planning Deployment of Interface Policies
 3. Switch Policies and Switch Policy Groups
 5. Profiles and Selectors
 1. Configuring Switch Profiles and Interface Profiles
 2. Stateless Networking in ACI
 6. Bringing It All Together
 1. Access Policies Hierarchy in Review
 2. Access Policies and Tenancy in Review
 7. Exam Preparation Tasks
 8. Review All Key Topics
 9. Complete Tables and Lists from Memory
 10. Define Key Terms
3. Chapter 7 Implementing Access Policies
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. Configuring ACI Switch Ports
 1. Configuring Individual Ports
 2. Configuring Port Channels

3. Configuring Virtual Port Channel (vPC) Domains
 4. Configuring Virtual Port Channels
 5. Configuring Ports Using AAEP EPGs
 6. Implications of Initial Access Policy Design on Capabilities
4. Configuring Access Policies Using Quick Start Wizards
 1. The Configure Interface, PC, and VPC Wizard
 2. The Configure Interface Wizard
5. Additional Access Policy Configurations
 1. Configuring Fabric Extenders
 2. Configuring Dynamic Breakout Ports
 3. Configuring Global QoS Class Settings
 4. Configuring DHCP Relay
 5. Configuring MCP
 6. Configuring Storm Control
 7. Configuring CoPP
 8. Modifying BPDU Guard and BPDU Filter Settings

9. Modifying the Error Disabled Recovery Policy
 10. Configuring Leaf Interface Overrides
 11. Configuring Port Channel Member Overrides
 6. Exam Preparation Tasks
 7. Review All Key Topics
 8. Complete Tables and Lists from Memory
 9. Define Key Terms
4. Chapter 8 Implementing Tenant Policies
1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. ACI Endpoint Learning
 1. Lookup Tables in ACI
 2. Local Endpoints and Remote Endpoints
 3. Understanding Local Endpoint Learning
 4. Unicast Routing and Its Impact on Endpoint Learning
 5. Understanding Remote Endpoint Learning
 6. Understanding the Use of VLAN IDs and VNIDs in ACI

7. Endpoint Movements Within an ACI Fabric
 8. Understanding Hardware Proxy and Spine Proxy
 9. Endpoint Learning Considerations for Silent Hosts
 10. Where Data Plane IP Learning Breaks Down
 11. Endpoint Learning on L3Outs
 12. Limiting IP Learning to a Subnet
 13. Understanding Enforce Subnet Check
 14. Disabling Data Plane Endpoint Learning on a Bridge Domain
 15. Disabling IP Data Plane Learning at the VRF Level
4. Packet Forwarding in ACI
 1. Forwarding Scenario 1: Both Endpoints Attach to the Same Leaf
 2. Understanding Pervasive Gateways
 3. Forwarding Scenario 2: Known Destination Behind Another Leaf
 4. Verifying the Traffic Path Between Known Endpoints
 5. Understanding Learning and Forwarding for vPCs

6. Forwarding Scenario 3: Spine Proxy to Unknown Destination
 7. Forwarding Scenario 4: Flooding to Unknown Destination
 8. Understanding ARP Flooding
5. Deploying a Multi-Tier Application
 1. Configuring Application Profiles, BDs, and EPGs
 2. Assigning Domains to EPGs
 3. Policy Deployment Following BD and EPG Setup
 1. Mapping EPGs to Ports Using Static Bindings
 2. Verifying EPG-to-Port Assignments
 3. Policy Deployment Following EPG-to-Port Assignment
 4. Mapping an EPG to All Ports on a Leaf
 5. Enabling DHCP Relay for a Bridge Domain
6. Whitelisting Intra-VRF Communications via Contracts
 1. Planning Contract Enforcement
 2. Configuring Filters for Bidirectional Application

1. Configuring Subjects for Bidirectional Application of Filters
 2. Understanding Apply Both Directions and Reverse Filter Ports
 3. Verifying Subject Allocation to a Contract
 4. Assigning Contracts to EPGs
 5. Understanding the TCP Established Session Rule
 6. Creating Filters for Unidirectional Application
 7. Configuring Subjects for Unidirectional Application of Filters
 8. Additional Whitelisting Examples
 9. Verifying Contract Enforcement
 10. Understanding the Stateful Checkbox in Filter Entries
 11. Contract Scopes in Review
-
7. Exam Preparation Tasks
 8. Review All Key Topics
 9. Complete Tables and Lists from Memory
 10. Define Key Terms

Part III External Connectivity

1. Chapter 9 L3Outs

1. “Do I Know This Already?” Quiz
2. Foundation Topics
3. L3Out Fundamentals
 1. Stub Network and Transit Routing
 2. Types of L3Outs
 3. Key Functions of an L3Out
 4. The Anatomy of an L3Out
 5. Planning Deployment of L3Out Node and Interface Profiles
 6. Understanding L3Out Interface Types
 7. Understanding L3Out Bridge Domains
 8. Understanding SVI Encap Scope
 9. Understanding SVI Auto State
10. Understanding Prerequisites for Deployment of L3Outs
11. L3 Domain Implementation Examples
12. Understanding the Need for BGP Route Reflection
13. Implementing BGP Route Reflectors

14. Understanding Infra MP-BGP Route Distribution
4. Deploying L3Outs
 1. Configuring an L3Out for EIGRP Peering
 2. Deploying External EPGs
 3. Verifying Forwarding Out an L3Out
 4. Advertising Subnets Assigned to Bridge Domains via an L3Out
 5. Enabling Communications over L3Outs Using Contracts
 6. Deploying a Blacklist EPG with Logging
 7. Advertising Host Routes Out an ACI Fabric
 8. Implementing BFD on an EIGRP L3Out
 9. Configuring Authentication for EIGRP
 10. EIGRP Customizations Applied at the VRF Level
 11. Configuring an L3Out for OSPF Peering
 12. A Route Advertisement Problem for OSPF and EIGRP L3Outs
 13. Implementing BFD on an OSPF L3Out
 14. OSPF Customizations Applied at the VRF Level

- [15. Adding Static Routes on an L3Out](#)
 - [16. Implementing IP SLA Tracking for Static Routes](#)
 - [17. Configuring an L3Out for BGP Peering](#)
 - [18. Implementing BGP Customizations at the Node Level](#)
 - [19. Implementing Per-Neighbor BGP Customizations](#)
 - [20. Implementing BFD on a BGP L3Out](#)
 - [21. Implementing BGP Customizations at the VRF Level](#)
 - [22. Implementing OSPF for IP Reachability on a BGP L3Out](#)
 - [23. Implementing Hot Standby Router Protocol \(HSRP\)](#)
 - [24. IPv6 and OSPFv3 Support](#)
- [5. Implementing Route Control](#)
 - [1. Route Profile Basics](#)
 - [2. Modifying Route Attributes to All Peers Behind an L3Out](#)
 - [3. Modifying Route Attributes to a Specific Peer Behind an L3Out](#)
 - [4. Assigning Different Policies to Routes at the L3Out Level](#)

5. Configuring Inbound Route Filtering in ACI
 6. Exam Preparation Tasks
 7. Review All Key Topics
 8. Complete Tables and Lists from Memory
 9. Define Key Terms
2. Chapter 10 Extending Layer 2 Outside ACI
1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. Understanding Network Migrations into ACI
 1. Understanding Network-Centric Deployments
 2. Understanding Full-Mesh Network-Centric Contracts
 3. Understanding Any EPG
 4. Understanding Preferred Group Members
 5. Disabling Contract Enforcement at the VRF Instance Level
 6. Flooding Requirements for L2 Extension to Outside Switches
 7. Understanding GARP-Based Detection
 8. Understanding Legacy Mode

9. Endpoint Learning Considerations for Layer 2 Extension
 10. Preparing for Network-Centric Migrations
4. Implementing Layer 2 Connectivity to Non-ACI Switches
 1. Understanding EPG Extensions
 2. Understanding Bridge Domain Extensions
 3. Comparing EPG Extensions and BD Extensions
 4. Implementing EPG Extensions
 5. Implementing L2Outs
 6. Migrating Overlapping VLANs into ACI
5. Understanding ACI Interaction with Spanning Tree Protocol
 1. Remediating Against Excessive Spanning Tree Protocol TCNs
 2. Configuring MST Instance Mappings in ACI
 3. Understanding Spanning Tree Protocol Link Types
 4. Using MCP to Detect Layer 2 Loops
6. Exam Preparation Tasks
7. Review All Key Topics

8. Complete Tables and Lists from Memory
9. Define Key Terms

Part IV Integrations

1. Chapter 11 Integrating ACI into vSphere Using VDS
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. Understanding Networking in VMware vSphere
 1. Understanding vSphere Standard Switches
 2. Understanding vSphere Distributed Switches
 3. Understanding vSphere System Traffic
 4. Impact of vCenter Failure on Production Traffic
 5. Understanding Port Bindings in vSphere
 6. Understanding Teaming and Failover Policies
 4. Understanding VMM Integration
 1. Planning vCenter VMM Integrations
 2. What Happens After VDS Deployment?

3. Understanding Immediacy Settings
 4. Connecting ESXi Servers to the Fabric
 5. Configuring Connectivity to ESXi in UCS Domains
 5. Integrating ACI into vSphere Using VDS
 1. Prerequisites for VMM Integration with vSphere VDS
 2. Configuring a VMM Domain Profile
 3. Adding ESXi Hosts to a VDS
 4. Pushing EPGs to vCenter as Distributed Port Groups
 5. Assigning VMs to Distributed Port Groups
 6. Less Common VMM Domain Association Settings
 7. Enhanced LACP Policy Support
 6. Exam Preparation Tasks
 7. Review All Key Topics
 8. Complete Tables and Lists from Memory
 9. Define Key Terms
2. Chapter 12 Implementing Service Graphs
 1. “Do I Know This Already?” Quiz

2. Foundation Topics
3. Service Graph Fundamentals
 1. Service Graphs as Concatenation of Functions
 2. Service Graph Management Models
 3. Understanding Network Policy Mode
 4. Understanding Service Policy Mode
 5. Understanding Service Manager Mode
 6. When to Use Service Graphs
 7. Choosing an L4-L7 Services Integration Method
 8. Understanding Deployment Modes and the Number of BDs Required
 9. Deploying Service Graphs for Devices in GoTo Mode
 10. Deploying Service Graphs for Devices in GoThrough Mode
 11. Deploying Service Graphs for One-Arm Load Balancers
 12. Understanding Route Peering
 13. Understanding Dynamic Endpoint Attach
 14. Understanding Bridge Domain Settings for Service Graphs

15. Understanding Service Graph Rendering

4. Service Graph Implementation Workflow

1. Importing Device Packages
2. Identifying L4-L7 Devices to the Fabric
3. Creating Custom Function Profiles
4. Configuring a Service Graph Template
5. Configuring Device Selection Policies
6. Applying a Service Graph Template
7. Configuring Additional Service Graph Parameters
8. Monitoring Service Graphs and Devices

5. Service Graph Implementation Examples

1. Deploying an Unmanaged Firewall Pair in a Service Graph
2. Deploying Service Graphs for a Firewall in Managed Mode

6. Exam Preparation Tasks

7. Review All Key Topics
8. Complete Tables and Lists from Memory
9. Define Key Terms

Part V Management and Monitoring

1. Chapter 13 Implementing Management

1. “Do I Know This Already?” Quiz
2. Foundation Topics
3. Configuring Management in ACI
 1. Understanding Out-of-Band Management Connectivity
 2. Understanding In-Band Management Connectivity
 3. Deploying In-Band and OOB Management Side by Side
 4. Configuring In-Band Management
 5. Configuring Access Policies for APIC In-Band Interfaces
 6. Configuring the In-Band Management Bridge Domain
 7. Configuring In-Band Management IP Addressing
 8. Optionally Extending the In-Band Network Out of the Fabric
 9. Optionally Setting Up Additional Connectivity
 10. Whitelisting Desired Connectivity to and from an In-Band EPG
 11. Evaluating APIC Connectivity Preferences

12. Out-of-Band Management Contracts in Review

4. Exam Preparation Tasks
5. Review All Key Topics
6. Memory Tables
7. Define Key Terms

2. Chapter 14 Monitoring ACI Using Syslog and SNMP

1. “Do I Know This Already?” Quiz
2. Foundation Topics
3. Understanding System Messages
4. Forwarding System Messages to Syslog Servers
 1. Apply Necessary Contracts to Allow Syslog Forwarding
 2. Configuring Syslog Monitoring Destination Groups
 3. Configuring Syslog Sources for Desired Monitoring Policies
 4. Verify Syslog Forwarding to Desired Syslog Servers
5. Using SNMP in ACI
 1. ACI Support for SNMP

2. ACI SNMP Configuration Caveats
 6. Configuring ACI for SNMP
 1. Apply Necessary Contracts for SNMP
 2. Associate an SNMP Policy with a Pod Policy
 3. Associate SNMP Contexts with Desired VRF Instances
 4. Configure SNMP Monitoring Destination Groups
 5. Configure SNMP Sources for All Desired Monitoring Policies
 6. Verify SNMP Forwarding to Desired SNMP Servers
 7. Exam Preparation Tasks
 8. Review All Key Topics
 9. Complete Tables and Lists from Memory
 10. Define Key Terms
3. Chapter 15 Implementing AAA and RBAC
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. Implementing Role-Based Access Control (RBAC)

1. Understanding Security Domains
 2. Understanding Privileges and Roles
 3. Creating Local Users and Assigning Access
 4. Tweaking Roles and User Access
 5. Custom RBAC Rules
 6. A Common RBAC Pitfall
4. Integrating with External AAA Servers
 1. Configuring ACI for TACACS+
 2. Configuring ISE to Authenticate and Authorize Users for ACI
 3. Expected Cisco AV Pair Formatting for ACI
 4. Configuring ACI for RADIUS
 5. Configuring ACI for LDAP
 6. AAA Authentication Policy Settings
 7. Regaining Access to the Fabric via Fallback Domain
5. Exam Preparation Tasks
6. Review All Key Topics
7. Complete Tables and Lists from Memory
8. Define Key Terms

Part VI Operations

1. Chapter 16 ACI Anywhere
 1. “Do I Know This Already?” Quiz
 2. Foundation Topics
 3. ACI Multi-Site Fundamentals
 1. Interconnecting ACI Fabrics with ACI Multi-Site
 2. New ACI Multi-Site Constructs and Configuration Concepts
 3. Locally Governed Versus MSO-Governed Configurations
 4. Schemas and Templates in Practice
 4. Building Primary and Disaster Recovery Data Centers with ACI
 1. Centralized Orchestration and Management of Multiple Fabrics
 2. Tweaking Broadcast and Stretch Settings on a Per-BD Basis
 3. Cross-Data Center Ingress Routing Optimizations
 4. Simultaneous or Independent Policy Deployment to Sites
 5. Building Active/Active Data Centers with ACI

1. VMM Integrations Applicable to Multiple Data Centers
2. Stateful-Services Integration in ACI Multi-Pod and Multi-Site
6. Extending ACI to Remote Locations and Public Clouds
 1. Extending ACI into Public Clouds with ACI Multi-Site
 2. Extending ACI into Bare-Metal Clouds with vPod
 3. Integrating Remote Sites into ACI Using Remote Leaf Switches
7. Exam Preparation Tasks
8. Review All Key Topics
9. Memory Tables
10. Define Key Terms

Part VII Final Preparation

1. Chapter 17 Final Preparation
 1. Getting Ready
 2. Tools for Final Preparation
 1. Pearson Cert Practice Test Engine and Questions on the Website

2. Accessing the Pearson Test Prep Software Online
 3. Accessing the Pearson Test Prep Software Offline
 4. Customizing Your Exams
 5. Updating Your Exams
 6. Premium Edition
3. Suggested Plan for Final Review/Study
4. Summary

Appendix A Answers to the “Do I Know This Already?” Questions

Appendix B CCNP Data Center Application Centric Infrastructure DCACI 300-620 Exam Updates

1. Always Get the Latest at the Book’s Product Page
2. Technical Content

Glossary

Index

Appendix C Memory Tables

Appendix D Memory Tables Answer Key

Appendix E Study Planner

Where are the companion content files? - Register

Inside Front Cover

Inside Back Cover

Code Snippets

1. i

2. ii

3. iii

4. iv

5. v

6. vi

7. vii

8. viii

9. ix

10. x

11. xi

12. xii

13. xiii

14. xiv

15. xv

16. xvi

17. xvii

18. xviii

19. xix

20. xx

21. xxi

22. xxii

23. xxiii

24. xxiv

25. xxv

26. xxvi

27. xxvii

28. xxviii

29. xxix

30. xxx

31. xxxi

32. xxxii

33. xxxiii

34. 2

35. 3

36. 4

37. 5

38. 6

39. 7

40. 8

41. 9

42. 10

43. 11

44. 12

45. 13

46. 14

47. 15

48. 16

49. 17

50. 18

51. 19

52. 20

53. 21

54. 22

55. 23

56. 24

57. 25

58. [26](#)

59. [27](#)

60. [28](#)

61. [29](#)

62. [30](#)

63. [31](#)

64. [32](#)

65. [33](#)

66. [34](#)

67. [35](#)

68. [36](#)

69. [37](#)

70. [38](#)

71. [39](#)

72. [40](#)

73. [41](#)

74. [42](#)

75. [43](#)

76. [44](#)

77. [45](#)

78. 46

79. 47

80. 48

81. 49

82. 50

83. 51

84. 52

85. 53

86. 54

87. 55

88. 56

89. 57

90. 58

91. 59

92. 60

93. 61

94. 62

95. 63

96. 64

97. 65

98. [66](#)

99. [67](#)

100. [68](#)

101. [69](#)

102. [70](#)

103. [71](#)

104. [72](#)

105. [73](#)

106. [74](#)

107. [75](#)

108. [76](#)

109. [77](#)

110. [78](#)

111. [79](#)

112. [80](#)

113. [81](#)

114. [82](#)

115. [83](#)

116. [84](#)

117. [85](#)

118. [86](#)

119. [87](#)

120. [88](#)

121. [89](#)

122. [90](#)

123. [91](#)

124. [92](#)

125. [93](#)

126. [94](#)

127. [95](#)

128. [96](#)

129. [97](#)

130. [98](#)

131. [99](#)

132. [100](#)

133. [101](#)

134. [102](#)

135. [103](#)

136. [104](#)

137. [105](#)

138. [106](#)

139. [107](#)

140. [108](#)

141. [109](#)

142. [110](#)

143. [111](#)

144. [112](#)

145. [113](#)

146. [114](#)

147. [115](#)

148. [116](#)

149. [117](#)

150. [118](#)

151. [119](#)

152. [120](#)

153. [121](#)

154. [122](#)

155. [123](#)

156. [124](#)

157. [125](#)

158. [126](#)

159. [127](#)

160. [128](#)

161. [129](#)

162. [130](#)

163. [131](#)

164. [132](#)

165. [133](#)

166. [134](#)

167. [135](#)

168. [136](#)

169. [137](#)

170. [138](#)

171. [139](#)

172. [140](#)

173. [141](#)

174. [142](#)

175. [143](#)

176. [144](#)

177. [145](#)

178. [146](#)

179. [147](#)

180. [148](#)

181. [149](#)

182. [150](#)

183. [151](#)

184. [152](#)

185. [153](#)

186. [154](#)

187. [155](#)

188. [156](#)

189. [157](#)

190. [158](#)

191. [159](#)

192. [160](#)

193. [161](#)

194. [162](#)

195. [163](#)

196. [164](#)

197. [165](#)

198. [166](#)

199. [167](#)

200. [168](#)

201. [169](#)

202. [170](#)

203. [171](#)

204. [172](#)

205. [173](#)

206. [174](#)

207. [175](#)

208. [176](#)

209. [177](#)

210. [178](#)

211. [179](#)

212. [180](#)

213. [181](#)

214. [182](#)

215. [183](#)

216. [184](#)

217. [185](#)

218. [186](#)

219. [187](#)

220. [188](#)

221. [189](#)

222. [190](#)

223. [191](#)

224. [192](#)

225. [193](#)

226. [194](#)

227. [195](#)

228. [196](#)

229. [197](#)

230. [198](#)

231. [199](#)

232. [200](#)

233. [201](#)

234. [202](#)

235. [203](#)

236. [204](#)

237. [205](#)

238. [206](#)

239. [207](#)

240. [208](#)

241. [209](#)

242. [210](#)

243. [211](#)

244. [212](#)

245. [213](#)

246. [214](#)

247. [215](#)

248. [216](#)

249. [217](#)

250. [218](#)

251. [219](#)

252. [220](#)

253. [221](#)

254. [222](#)

255. [223](#)

256. [224](#)

257. [225](#)

258. [226](#)

259. [227](#)

260. [228](#)

261. [229](#)

262. [230](#)

263. [231](#)

264. [232](#)

265. [233](#)

266. [234](#)

267. [235](#)

268. [236](#)

269. [237](#)

270. [238](#)

271. [239](#)

272. [240](#)

273. [241](#)

274. [242](#)

275. [243](#)

276. [244](#)

277. [245](#)

278. [246](#)

279. [247](#)

280. [248](#)

281. [249](#)

282. [250](#)

283. [251](#)

284. [252](#)

285. [253](#)

286. [254](#)

287. [255](#)

288. [256](#)

289. [257](#)

290. [258](#)

291. [259](#)

292. [260](#)

293. [261](#)

294. [262](#)

295. [263](#)

296. [264](#)

297. [265](#)

298. [266](#)

299. [267](#)

300. [268](#)

301. [269](#)

302. [270](#)

303. [271](#)

304. [272](#)

305. [273](#)

306. [274](#)

307. [275](#)

308. [276](#)

309. [277](#)

310. [278](#)

311. [279](#)

312. [280](#)

313. [281](#)

314. [282](#)

315. [283](#)

316. [284](#)

317. [285](#)

318. [286](#)

319. [287](#)

320. [288](#)

321. [289](#)

322. [290](#)

323. [291](#)

324. [292](#)

325. [293](#)

326. [294](#)

327. [295](#)

328. [296](#)

329. [297](#)

330. [298](#)

331. [299](#)

332. [300](#)

333. [301](#)

334. [302](#)

335. [303](#)

336. [304](#)

337. [305](#)

338. [306](#)

339. [307](#)

340. [308](#)

341. [309](#)

342. [310](#)

343. [311](#)

344. [312](#)

345. [313](#)

346. [314](#)

347. [315](#)

348. [316](#)

349. [317](#)

350. [318](#)

351. [319](#)

352. [320](#)

353. [321](#)

354. [322](#)

355. [323](#)

356. [324](#)

357. [325](#)

358. [326](#)

359. [327](#)

360. [328](#)

361. [329](#)

362. [330](#)

363. [331](#)

364. [332](#)

365. [333](#)

366. [334](#)

367. [335](#)

368. [336](#)

369. [337](#)

370. [338](#)

371. [339](#)

372. [340](#)

373. [341](#)

374. [342](#)

375. [343](#)

376. [344](#)

377. [345](#)

378. [346](#)

379. [347](#)

380. [348](#)

381. [349](#)

382. [350](#)

383. [351](#)

384. [352](#)

385. [353](#)

386. [354](#)

387. [355](#)

388. [356](#)

389. [357](#)

390. [358](#)

391. [359](#)

392. [360](#)

393. [361](#)

394. [362](#)

395. [363](#)

396. [364](#)

397. [365](#)

398. [366](#)

399. [367](#)

400. [368](#)

401. [369](#)

402. [370](#)

403. [371](#)

404. [372](#)

405. [373](#)

406. [374](#)

407. [375](#)

408. [376](#)

409. [377](#)

410. [378](#)

411. [379](#)

412. [380](#)

413. [381](#)

414. [382](#)

415. [383](#)

416. [384](#)

417. [385](#)

418. [386](#)

419. [387](#)

420. [388](#)

421. [389](#)

422. [390](#)

423. [391](#)

424. [392](#)

425. [393](#)

426. [394](#)

427. [395](#)

428. [396](#)

429. [397](#)

430. [398](#)

431. [399](#)

432. [400](#)

433. [401](#)

434. [402](#)

435. [403](#)

436. [404](#)

437. [405](#)

438. 406

439. 407

440. 408

441. 409

442. 410

443. 411

444. 412

445. 413

446. 414

447. 415

448. 416

449. 417

450. 418

451. 419

452. 420

453. 421

454. 422

455. 423

456. 424

457. 425

458. [426](#)

459. [427](#)

460. [428](#)

461. [429](#)

462. [430](#)

463. [431](#)

464. [432](#)

465. [433](#)

466. [434](#)

467. [435](#)

468. [436](#)

469. [437](#)

470. [438](#)

471. [439](#)

472. [440](#)

473. [441](#)

474. [442](#)

475. [443](#)

476. [444](#)

477. [445](#)

478. [446](#)

479. [447](#)

480. [448](#)

481. [449](#)

482. [450](#)

483. [451](#)

484. [452](#)

485. [453](#)

486. [454](#)

487. [455](#)

488. [456](#)

489. [457](#)

490. [458](#)

491. [459](#)

492. [460](#)

493. [461](#)

494. [462](#)

495. [463](#)

496. [464](#)

497. [465](#)

498. [466](#)

499. [467](#)

500. [468](#)

501. [469](#)

502. [470](#)

503. [471](#)

504. [472](#)

505. [473](#)

506. [474](#)

507. [475](#)

508. [476](#)

509. [477](#)

510. [478](#)

511. [479](#)

512. [480](#)

513. [481](#)

514. [482](#)

515. [483](#)

516. [484](#)

517. [485](#)

518. [486](#)

519. [487](#)

520. [488](#)

521. [489](#)

522. [490](#)

523. [491](#)

524. [492](#)

525. [493](#)

526. [494](#)

527. [495](#)

528. [496](#)

529. [497](#)

530. [498](#)

531. [499](#)

532. [500](#)

533. [501](#)

534. [502](#)

535. [503](#)

536. [504](#)

537. [505](#)

538. [506](#)

539. [507](#)

540. [508](#)

541. [509](#)

542. [510](#)

543. [511](#)

544. [512](#)

545. [513](#)

546. [514](#)

547. [515](#)

548. [516](#)

549. [517](#)

550. [518](#)

551. [519](#)

552. [520](#)

553. [521](#)

554. [522](#)

555. [523](#)

556. [524](#)

557. [525](#)

558. [526](#)

559. [527](#)

560. [528](#)

561. [529](#)

562. [530](#)

563. [531](#)

564. [532](#)

565. [533](#)

566. [534](#)

567. [535](#)

568. [536](#)

569. [537](#)

570. [538](#)

571. [539](#)

572. [540](#)

573. [541](#)

574. [542](#)

575. [543](#)

576. [544](#)

577. [545](#)

578. [546](#)

579. [547](#)

580. [548](#)

581. [549](#)

582. [550](#)

583. [551](#)

584. [552](#)

585. [553](#)

586. [554](#)

587. [555](#)

588. [556](#)

589. [557](#)

590. [558](#)

591. [559](#)

592. [560](#)

593. [561](#)

594. [562](#)

595. [563](#)

596. [564](#)

597. [565](#)

598. [566](#)

599. [567](#)

600. [568](#)

601. [569](#)

602. [570](#)

603. [571](#)

604. [572](#)

605. [573](#)

606. [574](#)

607. [575](#)

608. [576](#)

609. [577](#)

610. [578](#)

611. [579](#)

612. [580](#)

613. [581](#)

614. [582](#)

615. [583](#)

616. [584](#)

617. [585](#)

618. [586](#)

619. [587](#)

620. [588](#)

621. [589](#)

622. [590](#)

623. [591](#)

624. [592](#)

625. [593](#)

626. [594](#)

627. [595](#)

628. [596](#)

629. [597](#)

630. [598](#)

631. [599](#)

632. [600](#)

633. [601](#)

634. [602](#)

635. [603](#)

636. [604](#)

637. [605](#)

638. [606](#)

639. [607](#)

640. [608](#)

641. [609](#)

642. [610](#)

643. [611](#)

644. [612](#)

645. [613](#)

646. [614](#)

647. [615](#)

648. [616](#)

649. [617](#)

650. [618](#)

651. [619](#)

652. [620](#)

653. [621](#)

654. [622](#)

655. [623](#)

656. [624](#)

657. [625](#)

658. [626](#)

659. [627](#)

660. [628](#)

661. [629](#)

662. [630](#)

663. [631](#)

664. [632](#)

665. [633](#)

666. [634](#)

667. [635](#)

668. [636](#)

669. [637](#)

670. [638](#)

671. [639](#)

672. [640](#)

673. [641](#)

674. [642](#)

675. [643](#)

676. [644](#)

677. [645](#)

678. [646](#)

679. [647](#)

680. [648](#)

681. [649](#)

682. [650](#)

683. [651](#)

684. [652](#)

685. [653](#)

686. [654](#)

687. [655](#)

688. [656](#)

689. [C-2](#)

690. [C-3](#)

691. [C-4](#)

692. [C-5](#)

693. [C-6](#)

694. [C-7](#)

695. [C-8](#)

696. [C-9](#)

697. [C-10](#)

698. C-11

699. C-12

700. C-13

701. C-14

702. C-15

703. C-16

704. C-17

705. C-18

706. C-19

707. D-2

708. D-3

709. D-4

710. D-5

711. D-6

712. D-7

713. D-8

714. D-9

715. D-10

716. D-11

717. D-12

718. D-13

719. D-14

720. D-15

721. D-16

722. D-17

723. D-18

724. D-19

725. E-1

726. E-2