Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Virtual machine installation and administration
- Server administration
- Switch and network administration

New and Changed Information

The following tables provide an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New and Changed Behavior in Cisco ACI, Release 3.1(2m)

Feature	Description	Where Documented
Maximum MTU Increased	Up to Cisco APIC Release 3.1(2), the range is 576 to 9000 bytes. From release 3.1(2), and later, the maximum MTU value is 9216. The default has not changed from 9000.	*Provisioning Layer 3 Outside Connections*

Feature	Description	Where Documented
QoS for L3Out	QoS policy enforcement on L3Out ingress traffic is enhanced. To configure QoS policies in an L3Out, the VRF must be set in egress mode (Policy Control Enforcement Direction = "egress") with policy control enabled (Policy Control Enforcement Preference = "Enforced"). You must configure the QoS class priority or DSCP setting in the contract that governs the Layer 3 External network.	*Configuring Cisco ACI QoS*
Neighbor Discovery Router Advertisement on Layer 3 Out	RS/RA packets are used for auto configuration and are configurable on Layer 3 interfaces including routed interface, Layer 3 sub interface, and SVI.	*Provisioning Layer 3 Outside Connections*
BGP External Routed Network with Autonomous System Override	The AS override function replaces the AS number from the originating router with the AS number of the sending BGP router in the AS Path of the outbound routes.	*Provisioning Layer 3 Outside Connections*

Table 2: New and Changed Behavior in Cisco ACI, Release to 3.1(1i)

Feature	Description	Where Documented
Flood in Encapsulation	Beginning with Cisco ACI Release 3.1(1) on the Cisco ACI switches with the Application Spine Engine (ASE), all protocols are flooded in encapsulation. Multiple EPGs are now supported under one bridge domain with an external switch. When two EPGs share the same BD and the Flood in Encapsulation option is turned on, the EPG flooding traffic does not reach the other EPG. It overcomes the challenges of using the Cisco ACI switches with the Virtual Connect (VC) tunnel network.	Configuring Flood on Encapsulation Using the REST API

Feature	Description	Where Documented
Remote Leaf Switches	With an ACI fabric deployed, you can extend ACI services and APIC management to remote datacenters with Cisco ACI leaf switches that have no local spine switch or APIC attached.	*Remote Leaf Switches* in *Provisioning Layer 3 Outside Connections*
New Hardware Support for Multipod and GOLF	Multipod and GOLF are supported by all Cisco Nexus 9300 platform ACI-mode switches and all of the Cisco Nexus 9500 platform ACI-mode switch line cards and fabric modules. With Cisco APIC, release 3.1(x) and higher, this includes the N9K-C9364C switch.	*Cisco ACI GOLF* and *Multipod* in *Part 3, Provisioning Layer 3 Outside Connections*
Switch Virtual Interface (SVI) Auto State	Allows for the SVI auto state behavior to be enabled. This allows the SVI state to be in the down state when all the ports in the VLAN go down. This feature is available in the APIC Release 2.2(3x) release and going forward with APIC Release 3.1(1). It is not supported in APIC Release 3.0(x).	*Provisioning Layer 3 Outside Connections*
Layer 3 Multicast support with FEX	Multicast sources or receivers connected to FEX ports are supported.	*IP Multicast*
Tracking service nodes with Policy Based Redirect. IP SLA monitoring is supported.	With this release, Policy Based Redirect (PBR) supports tracking service nodes. This feature is available in the APIC Release 2.2(3x) release and going forward with APIC Release 3.1(1). It is not supported in APIC Release 3.0(x).	*Managing Layer 4 to Layer 7 Services*
ICMP or TCP protocol types are now used to track the Redirect Destination node.	ICMP or TCP protocol types are now used to track the Redirect Destination node. Only TCP was supported earlier.	*Managing Layer 4 to Layer 7 Services*

Feature	Description	Where Documented
Location-aware Policy Based Redirect	When you enable location aware redirection, and Pod IDs are specified, all the redirect destinations in the Layer 4-Layer 7 PBR policy will have pod awareness.	*Managing Layer 4 to Layer 7 Services*
MACsec	MACsec provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.	*Provisioning Layer 2 Networking*
CoPP per interface per protocol	Support for configuring CoPP on a per interface per protocol basis.	*Enabling Control Plane Policing*
BFD support for spine switch	Support for Bidirectional Forwarding Detection (BFD) on spine switch is added.	*Configuring BFD*

Note NOTE: The APIC Release 2.2(3x) feature is only available in this specific release. It is not supported in APIC Release 3.0(x) or Release 3.1(x).

Table 3: New and Changed Behavior in Cisco ACI, Release 2.2(3x)

Feature	Description	Where Documented
Switch Virtual Interface (SVI) Auto State	Allows for the SVI auto state behavior to be enabled. This allows the SVI state to be in the down state when all the ports in the VLAN go down.	*Provisioning Layer 3 Outside Connections*
Tracking service nodes with Policy Based Redirect.	With this release, the Policy Based Redirect feature (PBR) supports tracking service nodes with specific hashing algorithms.	*Managing L4-L7 Services*

Table 4: New and Changed Behavior in Cisco ACI, Release 3.0(1k)

Feature	Description	Where Documented
Forwarding Scale Profile Policy	The forwarding scale profile policy enables you to choose between Dual Stack (the default profile) and IPv4 Scale. A forwarding scale profile policy that is set to Dual Stack provides scalability of up to 6K endpoints for IPv6 configurations and up to 12K endpoints for IPv4 configurations. The IPv4 Scale option enables systems with no IPv6 configurations to increase scalability with up to 24K IPv4 endpoints.	*Configuring a Forwarding Scale Profile Policy*
Graceful Insertion and Removal (GIR) Mode	The Graceful Insertion and Removal (GIR) mode or maintenance mode allows you to isolate a switch from the network with minimum service disruption.	*Graceful Insertion and Removal (GIR) Mode*
Q-in-Q Encapsulation Mapping for EPGs	Using Cisco APIC, you can map double-tagged VLAN traffic ingressing on a regular interface, PC, or VPC to an EPG. When this feature is enabled, when double-tagged traffic enters the network for an EPG, both tags are processed individually in the fabric and restored to double-tags when egressing the ACI switch. Ingressing single-tagged and untagged traffic is dropped.	*Q-in-Q Encapsulation Mapping for EPGs*
First Hop Security	Enables better IPv4 and IPv6 link security and management over the layer 2 links.	*Configuring First Hop Security*
Latency and PTP	Latency is measured between endpoint groups, which requires all nodes in the fabric to be synchronized using the PTP protocol.	Troubleshooting Using Atomic Counters

Feature	Description	Where Documented
Enforced Bridge Domain	The configuration of an enforced bridge domain is supported, in which an endpoint in a subject endpoint group (EPG) can only ping subnet gateways within the associated bridge domain. With this configuration enabled, you can create a global exception list of IP addresses which can ping any subnet gateway.	*Enforced Bridge Domain* in *Configuring Tenant Policies*
Configuring BGP Max Path	Enables you to configure the maximum number of paths that BGP adds to the route table to invoke equal-cost multipath load balancing	*Configuring BGP Max Path* in *Provisioning Layer 3 Outside Connections*
AS Path Prepend	Allows for the change to the length of the autonomous system path in a BGP route to invoke best-path selection by a remote peer	*AS Path Prepend* in *Provisioning Layer 3 Outside Connections*

Table 5: New and Changed Behavior in Cisco ACI, Release 2.3(1e)

Feature	Description	Where Documented
Cisco APIC Quota Management	Creates, deletes, and updates a quota management configuration which enables the administrator to limit what managed objects can be added under a given tenant or globally across tenants.	*Creating Quota Management* in *Part 3*
Contract Inheritance	To streamline associating contracts to new EPGs, you can now enable an EPG to inherit all the (provided/consumed) contracts associated directly to another EPG in the same tenant. Contract inheritance can be configured for application, microsegmented, L2Out, and L3Out EPGs. Any changes you make to the EPG contract master’s contracts, are received by the inheriting EPG.	See *Contract Inheritance* in *Configuring Tenant Policies* in *Part 3*

Feature	Description	Where Documented
802.1Q Tunnels Enhancements	Now you can configure ports on core-switches for use in **Dot1q Tunnels** for multiple customers. You can also define access VLANs to distinguish between customers consuming the corePorts. You can also disable MAC learning on **Dot1q Tunnels**.	See *802.1Q Tunnels* in *Provisioning Layer 2 Networks* in *Part 3*
Reflective relay (802.1Qbg)	Reflective relay (802.1Qbg) transfers switching for virtual machines out of the host server to an external network switch. It provides connectivity between VMs on the same physical server and the rest of the network. It allows policies that you configure on the Cisco APIC to apply to traffic between the VMs on the same server.	See *Reflective relay (802.1Qbg)* in *Part 3*.
Control Plane Policing	Protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery.	See *Configuring Security* in *Part 3*
Encapsulation scope for SVI across Layer 3 Outside networks	With this release you can configure the encapsulation scope for SVI across Layer 3 Outside networks.	See *Provisioning Layer 3 Outside Connections* in *Part 3*.
Microsegmentation for virtual switches	Adds content for configuring microsegment EPGs on VMware VDS, Cisco AVS, and Microsoft vSwitch.	See *Configuring Microsegmentation on Virtual Switches* in *Part 3*.
Symmetric hashing	Symmetric hashing is now supported	See *Creating a Port Channel Policy Using the REST API*

Table 6: New Features and Changed Information in this Document for Cisco APIC 2.2(2e) release

Feature or Change	Description	Where Documented
Per VRF per node BGP timer values	With this release, you can define and associate BGP timers on a per VRF per node basis.	Provisioning Layer 3 Outside Connections
Layer 3 Out to Layer 3 Out Inter-VRF Leaking	With this release, shared Layer 3 Outs in different VRFs can communicate with each other using a contract.	Provisioning Layer 3 Outside Connections

Feature or Change	Description	Where Documented
Multiple BGP communities assigned per route prefix	With this release, multiple BGP communities can now be assigned per route prefix using the BGP protocol.	Entries for set additional communities are reflected in the code example in Managing Layer 3 Networking

Table 7: New Features and Changed Information in this Document

Feature or Change	Description	Where Documented
Name Change	Name of "Layer 3 EVPN Services for Fabric WAN" changed to "Cisco ACI GOLF"	*Cisco ACI GOLF* and *Multipod* in Provisioning Layer 3 Outside Connections

Table 8: New Features and Changed Information in this Document for Cisco APIC 2.2(1n) Release

Feature or Change	Description	Where Documented
Part 3: Setting Up APIC and the Fabric with the REST API	New section added.	Part 3
Managing Layer 4 to Layer 7 Services	Moved from Part 2 to Part 3	*Managing Layer 4 to Layer 7 Services* in *Setting up APIC and the Fabric with the REST API*
802.1Q Tunnels	You can now configure 802.1Q tunnels to enable point-to-multi-point tunneling of Ethernet frames in the fabric, with Quality of Service (QoS) priority settings.	*802.1Q Tunnels* in *Provisioning Layer 2 Networks*
APIC Cluster High Availability	Support is added to operate the APICs in a cluster in an Active/Standby mode. In an APIC cluster, the designated active APICs share the load and the designated standby APICs can act as an replacement for any of the APICs in an active cluster.	*Managing Cluster High Availability* in *Managing APIC Clusters*

Feature or Change	Description	Where Documented
Contract Preferred Groups	Support is added for contract preferred groups that enable greater control of communication between EPGs in a VRF. If most of the EPGs in the VRF should have open communication, but a few should only have limited communication with the other EPGs, you can configure a combination of a contract preferred group and contracts with filters to control communication precisely.	*Contract Preferred Groups* in *Configuring Tenants*
Dynamic Breakout Ports	Support is added for connecting a 40 Gigabit Ethernet (GE) leaf switch port to 4-10GE capable (downlink) devices (with Cisco 40-Gigabit to 4X10-Gigabit breakout cables).	*Dynamic Breakout Ports* in *Provisioning Layer 2 Networks*
FCoE over FEX Ports	You can now configure FCoE over FEX ports.	*Configuring FCoE over FEX Using the REST API* in *Provisioning Layer 2 Networks*
HSRP	Support is added for HSRP, a protocol that provides first-hop routing redundancy for IP hosts on Ethernet networks configured with a default router IP address.	*HSRP* in *Provisioning Layer 3 Outside Connections*
NetFlow	Support is added for NetFlow technology, which provides the metering base for a key set of applications, including network traffic accounting, usage-based network billing, network planning, as well as denial of services monitoring, network monitoring, outbound marketing, and data mining for both service providers and enterprise customers.	*NetFlow* in *Provisioning Core Services*

Table 9: New Features and Changed Information in this Document for Cisco APIC 2.1(1h) release

Feature or Change	Description	Where Documented
The document was created.		

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

⚠ **Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco Application Centric Infrastructure (ACI) Documentation

The ACI documentation is available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Simulator Documentation

The Cisco ACI Simulator documentation is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html.

Cisco Nexus 9000 Series Switches Documentation

The Cisco Nexus 9000 Series Switches documentation is available at http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html.

Cisco Application Virtual Switch Documentation

The Cisco Application Virtual Switch (AVS) documentation is available at http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation

Cisco ACI integration with OpenStack documentation is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.