Cisco ACI Long-Lived Release 5.2(x)

Contents

This document provides information about Cisco ACI long-lived release 5.2(x).

Date	Description
August 30, 2022	Added 5.2(6).
May 25, 2022	Added 5.2(5).
March 10, 2022	This document was published.

About Cisco ACI

The Cisco® Application Centric Infrastructure (Cisco ACI®) is part of our intent-based networking framework to enable agility in the datacenter. It captures higher-level business and user intent in the form of a policy and translates this into the network constructs necessary to dynamically provision network, security, and infrastructure services.

Built on top of the industry-leading Cisco Nexus® 9000 platform, Cisco ACI uses a holistic systems-based approach, with tight integration between hardware and software, between physical and virtual elements, an open ecosystem model, and innovative Cisco Application-Specific Integrated Circuits (ASICs) to enable unique business value for modern data centers.

Cisco ACI is the industry's most secure, open, and comprehensive Software-Defined Networking (SDN) solution.

Cisco ACI enables automation that accelerates infrastructure deployment and governance, simplifies management to easily move workloads across a multifabric, multicloud framework, and proactively secures against risk arising from anywhere. It radically simplifies, optimizes, and expedites the application deployment lifecycle.

Modern data centers are dynamic. IT operations must meet the expectation of quality-of-service business needs in a rapidly changing environment. Cisco ACI transforms IT operations from reactive to proactive with a highly intelligent set of software capabilities that analyzes every component of the data center to ensure business intent, guarantee reliability, and identify performance issues in the network before they happen.

As application usage gets more pervasive across an enterprise's network, IT professionals are looking to build solutions for consistent policy and encryption from the campus to the datacenter. With Cisco ACI integrations with SDA/DNA Center and SD-WAN, customers can now automate and extend policy, security, assurance, and insights across their entire networking ecosystem.

In this document, Cisco ACI followed by a release number represents Cisco APIC and Cisco Nexus 9000 series ACI-mode switches and their release numbers. For example, Cisco ACI 5.2(x) represents Cisco APIC, release 5.2(x) and Cisco Nexus 9000 series ACI-mode switches, release 15.2(x).

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco ACI Long-Lived Releases

Cisco ACI long-lived releases are software releases intended to help you stay on a given release on a long-term basis (up to approximately 18 months), while benefiting from frequent maintenance drops to ensure quality and stability. Cisco may support two long-lived releases at any given point of time. However, active maintenance will be focused primarily on the latest long-lived release. These releases will be maintained for a longer time span than other releases. Long-lived releases are recommended for the deployment of widely adopted functions or for networks that will not be upgraded frequently.

All long-lived releases support upgrade or downgrade to the next or previous long-lived release. See the Cisco APIC Upgrade/Downgrade Support Matrix for confirmed support. Some release branches might be supported as long-lived releases while others might not be supported. For example, there might be three 5.x release branches: 5.1, 5.2, and 5.3. However, one of the three 5.x release branches might be supported as a long-lived release (5.2), while the other two release branches (5.1 and 5.3) might not be supported as long-lived releases.

Figure 1 displays a visual example of recent long-lived release branch timelines.

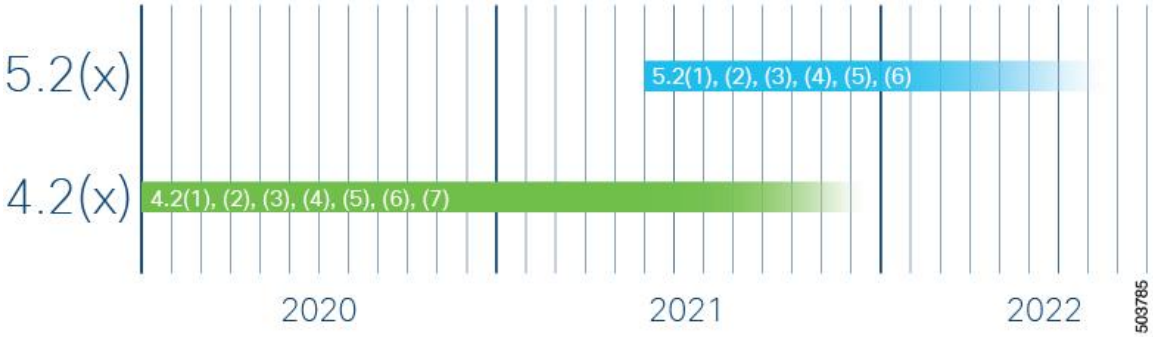

Figure 1. Example of Some Long-Lived Release Branch Timelines

Long-Lived Release Life Cycles

- The life cycle of a major long-lived release starts with the first customer shipment (FCS) of the first minor release.
- The major release then enters the maintenance release introduction phase, in which several releases are made available to address product defects.
- Afterward, the major release transitions to the mature maintenance phase. In this phase, the release receives defect resolutions only for severity 1 and severity 2 defects found by the customer. Defects found internally are addressed on a case-by-case basis.
- All long-lived releases support upgrade or downgrade to the next or previous long-lived release last maintenance version, respectively.

For additional information about long-lived releases, see the following:

- *Cisco APIC Installation, Upgrade, and Downgrade Guide*
- *Cisco APIC Upgrade Downgrade Support Matrix*
- *Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases*

Key Features in Release 5.2(x)

Feature name	Description	Release version
ACI-mode switch version and LLDP neighbors information	You can now view the ACI-mode switch release and information about LLDP neighbors of a node in the Cisco APIC GUI. To view this information: 1. On the menu bar, choose **Fabirc > Inventory**. 2. In the Navigation pane, choose **Fabric Membership**. 3. In the Work pane, choose the **Nodes Pending Registration** tab. 4. Double-click the row of a node. The information displays in the **General** tab of the dialog. The LLDP neighbor information includes the node ID, node name, node NX-OS version, and interfaces.	5.2(6)
Transport Layer Security version 1.3 support	Transport Layer Security (TLS) version 1.3 is now supported.	5.2(5)
DHCP server preference	When configuring a DHCP relay policy, you can now use the DHCP Server Preference option to select the administrative preference value for this provider. Using the value in this field, the leaf switch determines whether to route the DHCP relay packets from the client VRF or the server VRF. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).	5.2(4)
Dynamic L3Out EPG classification	The dynamic L3Out EPG classification (DEC) feature enables dynamic changes in pcTag with routing changes. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).	5.2(4)
Fallback route groups	This feature provides fast convergence for a destination that is reachable using a primary route and fallback route. You can group multiple next-hops of a route into one fallback route group so that if next-hop of the primary route fails, a Cisco ACI leaf switch can replace the failed primary next-hop with all the next-hops of the group in the hardware table before the control plane convergence with the routing protocol happens. This hardware-based convergence can happen within a second compared to multiple seconds or minutes for convergence through the control plane. In addition, next-hop failures can be detected faster through BFD. For more information, see the Configuring Fallback Route Groups document.	5.2(4)
Mis-cabling protocol strict mode	In strict mode, the mis-cabling protocol (MCP) checks for loops before allowing data traffic. Early loop detection is supported, and data traffic is blocked until the early loop detection process is complete. For more information, see the Cisco Application Centric Infrastructure Fundamentals, Releases 5.2(x).	5.2(4)
Route filtering and aggregation	There is now an option to summarize or filter routes that are advertised in a fabric to reduce the scale requirements of the fabric. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).	5.2(4)

Feature name	Description	Release version
Service EPG selector for endpoint security groups	The service EPG selector for endpoint security groups (ESGs) is now available. This feature allows you to map a service EPG to an ESG and create a contract with that ESG. Using this feature, even if you have a vzAny-to-vzAny permit contract that is configured, you can add a deny contract between the service ESG and other ESGs to allow specific ESGs to communicate with the service ESG. For more information, see the Cisco APIC Security Configuration Guide, Release 5.2(x).	5.2(4)
SSL option for the transport protocol for syslog messages	SSL is now an option for the transport protocol for syslog messages. This feature enables a Cisco ACI switch (acting as a client) to make a secure, encrypted outbound connection to remote syslog servers (acting as a server) supporting secure connectivity for logging. With authentication and encryption, this feature allows for a secure communication over an insecure network. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).	5.2(4)
Support for adding or replacing a Cisco ACI switch that reaches to the Cisco APIC cluster only through an IPN device with Cisco NXOS to Cisco ACI POAP auto-conversion	With Cisco ACI power-on auto-provisioning (POAP) auto-conversion, you can now add a Cisco NX-OS node as a new remote leaf node, add a Cisco NX-OS node as a first spine node in a new pod, replace a remote leaf node, or replace a spine node in a Cisco ACI Multi-Pod setup with only one spine node in the pod. For more information, see the Cisco APIC Getting Started Guide, Release 5.2(x)	5.2(4)
Support for BFD on secondary IPv4/IPv6 subnets	Bidirectional Forwarding Detection (BFD) is now supported for static routes that are reachable using secondary IPv4/IPv6 subnets that are configured on routed interfaces. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).	5.2(4)
Support for DHCPv6 option 79	Option 79 is now supported for DHCPv6, which provides the client's link layer address in the DHCPv6 messages that are sent toward the server. When a relay message from the client to the server contains the client identifier DUID and option 79, the server identifies the option 79 present in the solicit packet that is sent to the server for requesting an IP address. The IPv6 allocation is performed based on option 79 and not based on the DUID. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).	5.2(4)
Support for FIPS 140-2	The FIPS cryptographic functions have been updated to be compatible with current FIPS 140-2 requirements.	5.2(4)
Support for Smart License With Policy	The Cisco ACI Smart Licensing feature has been replaced by the Cisco ACI Smart License With Policy (SLP) feature. SLP is a software management platform that manages all Cisco product licenses. SLP simplifies license management compared to the original Cisco Smart Licensing feature. SLP provides a licensing solution that does not interrupt the operations of your network and enables a compliance relationship that considers the hardware and software licenses you purchase and use. For more information, see the Cisco ACI Smart Licensing With Policy	5.2(4)

Feature name	Description	Release version
Support for the same encapsulation for IPv4 and IPv6	You can now use the same encapsulation for IPv4 and IPv6. One port group is created for the IPv4 and IPv6 address families for the same L3Out with a VMM domain. While deploying a floating SVI, if both address families are configured under the L3Out, both floating SVIs for IPv4 and IPv6 are deployed on the leaf nodes. For more information, see the Using Floating L3Out to Simplify Outside Network Connections document.	5.2(4)
Support for vzAny for an Intersite L3Out	You can now enable vzAny contracts between a consumer VRF instance and L3Out external EPGs that are part of a different provider VRF instance. For more information, see the Cisco Multi-Site Configuration Guide for ACI Fabrics, Release 3.3(x).	5.2(4)
Synchronous Ethernet and PTP Telecom profile (G.8275.1) support on port channels	Synchronous Ethernet (SyncE) and the PTP Telecom profile (G.8275.1) are now supported on port channels. Cisco APIC System Management Configuration Guide, Release 5.2(x)	5.2(4)
BGP underlay for Cisco ACI Multi-Pod and remote leaf switches	The border gateway protocol (BGP) is now available as an alternative to the Open Shortest Path First (OSPF) protocol for the Inter-Pod Network (IPN) underlay. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).	5.2(3)
Cisco ACI Multi-Pod spine switches back-to-back	In some cases, two pods can now be interconnected directly ("back-to-back") without using an IPN device. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x) and Cisco ACI Multi-Pod Spines Back-to-Back document.	5.2(3)
Cisco NX-OS to Cisco ACI POAP auto-conversion	Cisco NX-OS to Cisco ACI power-on auto-provisioning (POAP) auto-conversion automates the process of upgrading software images and installing configuration files on nodes that are being deployed in the network for the first time. When a Cisco NX-OS node with the POAP auto-conversion feature boots and does not find the startup configuration, the node enters the POAP mode and starts DHCP discovery on all ports. The node locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The device also obtains the IP address of a TFTP server and downloads a configuration script that enables the node to download and install the appropriate software image and configuration file. This process converts the Cisco NX-OS node from the standalone mode to the Cisco ACI-mode. For more information, see the Cisco APIC Getting Started Guide, Release 5.2(x).	5.2(3)

Feature name	Description	Release version
Endpoint security group enhancements	Endpoint security groups (ESGs) now support more features and configurations, such as: • Inter-VRF service graphs between ESGs • ESG shutdown • Host-based routing/host route advertisement • ESGs can be specified as a source or destination of the following features: ◦ On Demand Atomic Counter ◦ On Demand Latency Measurement For the full list of newly-supported features and configurations, see the Cisco APIC Security Configuration Guide, Release 5.2(x).	5.2(3)
ERSPAN supports IPv6 destinations	ERSPAN now supports IPv6 destinations.	5.2(3)
Integrity check for exported configuration files that are saved on external servers	There is now an integrity check for exported configuration files that are saved on external servers, which ensures that the file's contents are not tampered with. For more information, see the Cisco ACI Configuration Files: Import and Export document.	5.2(3)
Micro Bidirectional Forwarding Detection	Micro Bidirectional Forwarding Detection (BFD) establishes individual BFD sessions on each member link of a port channel for faster failure detection and easier troubleshooting. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).	5.2(3)
Open Authorization 2.0 support	Open Authorization (OAuth) 2.0 is an open-standard authorization protocol. OAuth 2.0 allows you to access an application (Service Provider or SP) that is trusted or approved by an Identity Provider (IdP). OAuth 2.0 uses authorization tokens to provide identity and authorization claims to the consumer application. Beginning with Cisco APIC Release 5.2(3), OAuth 2 server can be used to set up an application (such as, Cisco APIC) as an identity server that authenticates users using single sign-on. For more information, see the Cisco APIC Security Configuration Guide, Release 5.2(x).	5.2(3)
Rogue/COOP exception list	The rogue/COOP exception list enables you to specify the MAC address of endpoints for which you want to have a higher tolerance for endpoint movement with rogue endpoint control before the endpoints get marked as rogue. Endpoints in the rogue/COOP exception list get marked as rogue only if they move 3000 or more times within 10 minutes. After an endpoint is marked as rogue, the endpoint is kept static to prevent learning. The rogue endpoint is deleted after 30 seconds. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).	5.2(3)
Security GUI screen enhancements	The security screens in the GUI are enhanced to show more information about the contract consumers and providers, and now include the ability to filter the data and view the resolved paths for an EPG or contract. For more information, see the online help pages for the **System > Security** and **Tenants > *tenant_name* > Security** screens.	5.2(3)

Feature name	Description	Release version
Specifying a transport protocol for a syslog remote destination	You can now specify a transport protocol to use for sending the syslog messages when you create a syslog remote destination. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).	5.2(3)
Support for Layer 3 multicast on L3Outs with SVI	Layer 3 multicast on an L3Out with SVI adds support for enabling PIM on L3Out SVIs. This allows the ACI border leaf switch configured with an L3Out SVI to establish PIM adjacencies with an external multicast router or firewall. For more information, see Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).	5.2(3)
Support for multiple encapsulations for L3Outs with SVI	Beginning with release 5.2(3), you can use different VLAN encapsulations for an external bridge domain for L3Outs configured with SVIs, where all of the different external encapsulation instances are treated as part of a single Layer 2 domain. Prior to release 5.2(3), L3Outs configured with SVIs are limited to one VLAN encapsulation for each external bridge domain. However, with the introduction of floating L3Outs in release 4.2(1), there are scenarios where multiple VLAN encapsulations are needed for the same external bridge domain. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x) and Using Floating L3Out to Simplify Outside Network Connections document.	5.2(3)
Support for Prometheus Node Exporter	Support is now available for monitoring metrics using the Prometheus Node Exporter. The Prometheus Node Exporter provides visibility to a wide variety of hardware and kernel-related metrics, where it collects technical information from Linux nodes, such as CPU, disk, and memory statistics. For more information, see the Monitoring Metrics Using the Prometheus Node Exporter document.	5.2(3)
time-range REST API query option for viewing log record objects	Beginning with Cisco APIC release 5.2(3), with the new API query option time-range that is supported only for log record objects, the Cisco APIC can respond to the API query for the log record objects much faster. The Cisco APIC GUI also uses the time-range option for improved performance. This new query option for log record objects are not used in the CLI commands such as show faults history or show events. For more information about the time-range option, see the Cisco APIC REST API Configuration Guide, Release 4.2(x) and Later. For information about log record objects and using the GUI to view the objects, see the Cisco Application Centric Infrastructure Fundamentals, Releases 5.2(x).	5.2(3)
USB port on Cisco ACI-mode switches can be disabled	You can now disable the USB port on a Cisco ACI-mode switch. If you have disabled the USB port, then when the switch is rebooted, the switch boots using the last known operating system image in the bootflash instead of using an image on a connected USB device. This feature provides an extra layer of protection in the event that someone power cycles the switch to try to boot the switch from a USB image that contains malicious code. For more information, see the Disabling the USB Port on Cisco ACI-Mode Switches document.	5.2(3)
Alias, Annotations, and Tags	Several methods are provided for adding label metadata to objects.	5.2(1)

Feature name	Description	Release version
Automatic FPGA/EPLD/BIOS upgrade	Switches will automatically upgrade the FPGA/EPLD/BIOS based on the booting ACI switch image during a normal boot-up sequence for certain components, even if it's not an upgrade operation performed through the APICs.	5.2(1)
Disabling dataplane IP address learning per endpoint or subnet	You can disable dataplane IP address learning per endpoint or subnet. Previously, you could only disable dataplane IP address learning per VRF instance or bridge domain.	5.2(1)
Dynamic MAC address detection for a Layer 3 policy-based redirect destination	You can configure any of the Layer 3 policy-based redirect (PBR) destinations without specifying a MAC address, which causes the leaf switches to use the Address Resolution Protocol (ARP) to determine the MAC address of the PBR next-hop. The benefit is that you do not need to check the MAC address of each PBR destination and an active-standby HA pair does not need to use a floating MAC address.	5.2(1)
End of support for device packages	Device packages are no longer supported. There is no longer a managed mode for devices; all devices are effectively unmanaged.	5.2(1)
EPG and tag selectors for ESGs	Endpoint group (EPG) selectors can add specific EPGs to an endpoint security group (ESG). Tag selectors can add objects to an ESG based on policy tags.	5.2(1)
HTTP URI tracking	You can track service nodes using the HTTP URI.	5.2(1)
MACsec support on N9K-X9716D-GX	MACsec is now supported on the Cisco N9K-X9716D-GX line card.	5.2(1)
Next-hop propagation with OSPF and static routes redistributed in BGP for floating L3Outs	Next-hop propagation is supported with OSPF and static routes redistributed in BGP for floating L3Outs.	5.2(1)
Policy-based redirect destination in an L3Out	A policy-based redirect destination can now be in an L3Out.	5.2(1)
Remote leaf peer-link support	Connect pairs of remote leaf switches directly to each other ("back-to-back") by fabric links to carry local east-west traffic.	5.2(1)
Simplified ESG migration	EPG to ESG migration is simplified using EPG selectors.	5.2(1)
Site-of-Origin (SoO)	The SoO is a BGP extended community attribute that uniquely identifies the site from which a route is learned in order to prevent routing loops.	5.2(1)
Software Maintenance Upgrade Patches	You can install software maintenance upgrade (SMU) patches that contain fixes for specific defects. Because SMU patches can be released much more quickly than a more traditional patch release, you can resolve specific issues in a more timely manner.	5.2(1)
Cisco APIC cluster connectivity to the fabric over a Layer 3 network	Support for a topology in which the Standalone APIC cluster is separated from the ACI fabric by a Layer3 inter-pod network (IPN).	5.2(1)

Feature name	Description	Release version
Support for intra-EPG contracts on L3Out EPGs	Intra-EPG contracts are supported on L3Out EPGs. The action can be permit, deny, or redirect.	5.2(1)
Support for multiple next-hops to be propagated in the Cisco ACI fabric for redistributed routes in BGP for floating L3Outs	Support for multiple next-hops to be propagated in the ACI fabric for redistributed routes in BGP for floating L3Outs.	5.2(1)
Support for Telecom PTP profile (G.8275.1)	The Telecom PTP profile (G.8275.1) is now supported.	5.2(1)
Synchronous Ethernet (SyncE)	Distributes high-quality clock frequency synchronization over Ethernet ports.	5.2(1)
VMware enhanced LACP support for virtual Layer4 to Layer7 devices	Support for enhanced LACP on interfaces of Layer4 to Layer7 virtual service devices used in service graphs.	5.2(1)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 01/21