Cisco IOS XR Release 6.1.2 for Cisco ASR 9000 Series Routers

PB737145

Product Overview

Cisco® ASR 9000 Series Aggregation Services Routers (ASR 9000 Series) deliver unprecedented scale, service flexibility, and high availability for service providers' fixed and mobile networks, data centers, and transport networks. The routers are powered by Cisco IOS® XR Software, an innovative, self-healing, distributed operating system designed for always-on operation while scaling system capacity into multiple terabits per second (Tbps).

Cisco IOS XRv 9000 is a virtual router that runs the Cisco IOS XR Software 64-bit operating system on generic x86-based hardware. It is provided as a virtual machine, supporting full virtualization that can be deployed on any x86 hardware running standard hypervisors. The Cisco IOS XRv router supports the same control-plane features and configurations that are supported on the Cisco ASR 9000 Series and Cisco CRS Routers.

New Hardware Features

The Cisco IOS XR Software Release 6.1.2 introduces support for a new modular 400G consumption model line card.

Table 1 lists the new hardware support that has been added to Cisco IOS XR Software Release 6.1.2.

Table 1.   New Hardware Supported on Cisco ASR 9000 Series Routers in Cisco IOS XR Software Release 6.1.2

PID	Description
A9K-MOD400-CM	ASR 9000 Modular 400G Consumption Model Line Card
A9K-MOD400-CM=	ASR 9000 Modular 400G Consumption Model Line Card (Spare)
A9K-MPA20X10GE-CM	ASR 9000 20x10GE Consumption Model MPA
A9K-MPA20X10GE-CM=	ASR 9000 20x10GE Consumption Model MPA (Spare)
A9K-MPA2X100GE-CM	ASR 9000 2x100GE Consumption Model MPA
A9K-MPA2X100GE-CM=	ASR 9000 2x100GE Consumption Model MPA (Spare)
A9K-MOD400-CM	ASR 9000 Modular 400G Consumption Model Line Card
A9K-MOD400-CM=	ASR 9000 Modular 400G Consumption Model Line Card (Spare)
ASR-XRV9000-APLN	Cisco IOS XRV 9000 Appliance with UCS C220 M4 Server
ASR-XRV9000-APLN=	Cisco IOS XRV 9000 Appliance with UCS C220 M4 Server (Spare)

New Software Features

Table 2 lists new software features in Cisco IOS XR Software Release 6.1.2 supported on Cisco ASR 9000 Series Aggregation Services Routers.

Table 2.   New Software Features Supported on Cisco ASR 9000 Series Routers in Cisco IOS XR Software Release 6.1.2

Feature	Description
Cisco IOS XR Software 64-bit	**Fully automated initial installation** • Bootable ISO: To simplify installation, Cisco IOS XR Software 64-bit on ASR 9000 images are in the form of a bootable ISO that's installed on the system. The software also supports iPXE, which allows the administrator to boot from TFTP, HTTP, or FTP. • Auto-provisioning: Auto-provisioning starts at the end of the software's boot process and serves two functions: static configuration application and script execution. It allows administrators to customize settings easily and automatically, without wasting time on manual configuration. **Visibility for smarter control, simpler monitoring, and faster troubleshooting** • Streaming telemetry: Users can take advantage of streaming telemetry to direct data to a configured receiver. Data can be pushed out at intervals determined by the administrator, at a cadence as low as 10 seconds. Using sophisticated algorithms, a back-end server can then analyze data received from Cisco IOS XR Software 64 bit on ASR 9000. The data can be encoded in JavaScript Object Notation (JSON) or Google Protocol Buffers (GPB). This analysis enables back-end management systems to measure and even predict control-plane and data-plane trends. • Model Driven interfaces: Prior to Release 6.0, administrators relied on Simple Network Management Protocol (SNMP) and syslog—techniques that are neither scalable nor easily automated. With this latest release of Cisco IOS XR Software, administrators can more easily work together using the internal system database (SysDB) represented by YANG models. SysDB is not a database in a strict sense, but rather a tree-like file system that can provide a common mechanism for management clients to modify or access system information. SysDB stores a variety of types of data, including integers of different sizes, character strings, and externally managed data items. **Open architecture** Linux-based OS: Release 6.1.2 opens up the architecture of Cisco IOS XR Software using a 64-bit Linux-based operating system. (It uses the Wind River 7 distribution, which is compatible with Yocto 1.5 and approved by the Yocto project.) In contrast to the traditional 32-bit QNX OS, Release 6.1.2 can easily integrate applications, configuration-management tools, and autoprovisioning. These attributes make it highly automatable and transparent to monitoring and management tools. **In-Service Software Upgrade (ISSU)** In-Service Software Upgrade: Cisco IOS XR Software 64 bit on ASR 9000 will have new foundation for the In Service Software Upgrade. The virtualized environment to run instances of Cisco IOS XR Software 64 bit will enable the platform to provide capability to orchestra software upgrade process to minimize the disruption of the services in the network without powering down the system to upgrade the Cisco IOS XR Software 64 bit on ASR 9000. **Segmented Multicast Stitching with Inter AS support on Cisco IOS XR Software 64 bit** Segmented Multicast Stitching with Inter AS is now supported on Cisco IOS XR Software 64 bit. The segmented multicast stitching with Inter AS solution makes sure that the ABR and ASBR having an incoming core type is switched to a different or same core type. **MLDP Carrier Supporting Carrier Based MVPN support on Cisco IOS XR Software 64 bit** MLDP Carrier Supporting Carrier Based MVPN is now supported on Cisco IOS XR Software 64 bit. The MLDP carrier-supporting-carrier (CSC) feature enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. **Multicast VPN, MVPN over GRE and Multicast only Fast Reroute support on IOS XR 64 bit** Multicast VPN (MVPN), MVPN over GRE (MoGRE) and Multicast only Fast Reroute (MoFRR) features are now supported on Cisco IOS XR Software 64 bit. **Global Table Multicast support on Cisco IOS XR Software 64 bit** Layer 3 Global Table Multicast (GTM) is now supported on Cisco IOS XR Software 64 bit. Multicast routing information that is not specific to VPNs is stored in a router's "global table", rather than in a VRF and hence it is known as "Global Table Multicast". **Supported Platforms** The following Cisco platforms support Cisco IOS XR Software 64 bit on ASR 9000: • Cisco ASR 9000 Series routers with RSP800 or RP2 (both –SE and –TR) and the latest generation ASR 9000 Linecards, for example, A99-8X100GE-SE/-TR, A9K-8X100GE-SE/-TR, A9K-4X100GE-SE/-TR.
BNG Geo Redundancy Features	**Active-active Session Support for Geo Redundancy** Active-active session support for BNG geo redundancy is an enhancement where a subscriber redundancy group (SRG) can be primary on a BNG node while being secondary on the pair BNG node, and simultaneously another SRG can be primary on the pair BNG node while being secondary on the primary BNG node. So, a BNG node can be a primary for one SRG and at the same time secondary for another SRG. This feature provides better load balancing for subscriber sessions across both the BNG nodes. **State Control Route for Geo Redundancy** State control route is a loss-of-signal (LOS) based solution for BNG geo redundancy, where the route advertisement to the core network is controlled based on the role of the subscriber redundancy group (SRG). Only the summary routes from the primary SRG group get advertised to the core network; not the routes from the secondary SRG. When a switchover happens, the new secondary SRG withdraws the previously advertised routes from the core. This solution provides a sub-second traffic convergence and prevents traffic backhauling. This feature is mainly useful in BNG deployments where optical line terminals (OLTs) do not support access protocols (like BFDs, CFM and so on) to detect link failures in the access or core network.

Feature	Description
	Subscriber Redundancy Group Revertive Timer Subscriber redundancy group (SRG) revertive timer feature is an enhancement in BNG geo redundancy where, based on certain conditions, the primary BNG node for which the preferred role is set as primary, automatically regains the primary role (from secondary role) after an SRG fail over. An auto-revertive timer starts when the preferred primary BNG becomes secondary due to SRG fail over and when the access-tracking and core-tracking are restored. When the timer expires, the preferred primary BNG regains the primary role. This switch back to the preferred primary role is required, as the new primary SRG may not be equipped to handle the entire subscriber load in the case of a fail over. **Subscriber Redundancy Group-aware IPv6 Neighbor Discovery** Subscriber Redundancy Group-aware (SRG-aware) IPv6 Neighbor Discovery (ND) is an enhancement in BNG geo redundancy where, the Router Advertisement (RA) message in response to the IPv6 ND message for IPv6 deployments, is sent based on the SRG role of the parent interface. Only the primary node sends out RA message in response to IPv6 ND message and brings up the session. The RS (Router Solicitation) or Neighbor Solicitation (NS) message is dropped on the secondary node, but the sessions still come up in that secondary node. That way, the routes are not advertised to the core from the standby node. **Peer-to-peer Traffic Flow with BNG Geo Redundancy** Peer-to-peer traffic flow is an enhancement in BNG Geo Redundancy where subscribers in different subscriber redundancy groups (SRGs) in the primary and secondary nodes can send traffic to each other through the BNG nodes. This is feasible as the primary SRGs from both the BNG nodes advertise the respective summary routes to the core. **Accounting Trigger Cause for Geo Redundancy** A new Cisco-Attribute Value Pair (AVP), Acct-Trigger-Cause, is introduced to send the reason of accounting start and accounting stop messages triggered during an SRG switchover. The accounting stop record sent from the old primary BNG node and the accounting start record sent from the new primary BNG node, specifies the Acct-Trigger-Cause to be nas-switchover. This in turn helps the backend servers to identify the reason of the new accounting trigger thereby preventing the existing accounting records of the subscriber sessions from getting deleted. **BNG DIAMETER-Geo Redundancy Interworking** BNG extends the geo redundancy feature to support DIAMETER protocol for the northbound interfaces. DIAMETER being a stateful protocol, unlike RADIUS which is a stateless protocol, the northbound interface convergence with respect to the NASREQ, Gx and Gy applications is taken care in the case of BNG switchovers. This functionality is mainly useful for the back end servers to seamlessly maintain the subscriber accounting information of prepaid customers in the case of node fail overs.
BNG Smart Licensing	BNG supports Cisco Smart Software Licensing that provides a simplified way for the customers to purchase licenses and to manage them across their network. This provides a customizable consumption-based model that aligns to the network growth of the customer. It also provides the flexibility to quickly modify or upgrade software feature configurations to deploy new services over time.
BNG on High Density 100GE Ethernet Line Card	BNG support is extended to these Cisco ASR 9000 High Density 100GE Ethernet line cards: • 8-port 100GE, Service Edge Optimized Line Card • 8-port 100GE, Packet Transport Optimized Line Card
NSH Based Service Chaining	Network Services Header (NSH) is a technology to group ("service chain") different applications running on physical appliances or as virtualized loads. It decouples the service topology from the actual network topology, offering a unified data plane. NSH describes a sequence of service nodes that a packet must be routed prior to reaching its destination and adds this metadata information about the packet and/or service chain to an IP/MPLS packet. Support for this is included on the ASR9000 is included in this release.
Segment Routing	**Auto-route Destination** The auto-route destination feature allows you to automatically route traffic through a segment routing tunnel instead of manually configuring static routes. Static routes are always added with zero-cost metric, which can result in traffic that is mapped on multiple tunnels to always load-balance due to ECMP. This load-balancing may be undesirable when some of those tunnels have sub-optimal paths. With auto-route destination, only the tunnel whose IGP cost to its endpoint is lowest will be considered for carrying traffic. **Node and Shared Risk Link Groups Protection with Topology-Independent Loop-Free Alternate** The Topology-Independent Loop-Free Alternate (TI-LFA) node protection functionality provides protection from node failures. The neighbor node is excluded during the post convergence backup path calculation. The TI-LFA Shared Risk Link Groups (SRLG) protection functionality attempts to find the post-convergence backup path, which excludes the SRLGs of the protected link. All local links that share any SRLG with the protecting link are excluded during the post convergence backup path calculation. **Segment Routing Egress Peer Engineering** Segment routing egress peer engineering (EPE) uses a controller to instruct an ingress provider edge or a content source within the segment routing domain to use a specific egress provider edge and a specific external interface to reach a destination. BGP peer SIDs are used to express source-routed inter-domain paths. Controllers learn BGP peer SIDs and the external topology of the egress border router through BGP-LS EPE routes. EPE functionality is only required at EPE egress border router and EPE controller.

Feature	Description
XRv9000	**Multi-socket Dataplane** The Cisco IOS XRv 9000 router now supports scale up capability. With this feature a dataplane can now span across one or more sockets. **Network Service Header (NSH)** Network Service Header is the Service Function Chaining (SFC) encapsulation required to support the SFC Architecture (defined in RFC7665). The NSH is inserted onto ingress encapsulated packets or frames to realize service function paths. NSH also provides a mechanism for metadata exchange along the instantiated service path. **Link Bundle or Link Aggregation Group (LAG)** A link bundle is a group of one or more ports that are aggregated together and treated as a single link. Each bundle has a single MAC, a single IP address, and a single configuration set (such as ACLs). Since XRv 9000 is a virtual platform, you must configure mac address on each bundle main interface. Use **lacp system mac** command in global configuration mode and **mac address** command in interface configuration mode to configure mac address to bundle main interface. Link Aggregation Control Protocol (LACP) for virtual E1000 is not supported. **BFD over Logical Bundle (BLB)** BLB is a multipath (MP) single-hop session. BLB requires limited knowledge of the bundle interfaces on which the sessions run; this is because BFD treats the bundle as one big pipe. To function, BLB requires only **information** about IP addresses, interface types, and caps on bundle interfaces. Information such as list of bundle members, member states, and configured minimum or maximum bundle links are not required. **Application Hosting** Application hosting gives administrators a platform for using their own tools and utilities. Cisco XRv 9000 supports third-party off-the-shelf applications built using Linux tool chains. Users can run custom applications cross-compiled with the software development kit that Cisco provides. Application hosting is offered in two variants: Native and Container.
IP Routing and features	**Prefix Suppression for OSPF** Improved convergence and reduced vulnerability of potential remote attacks by suppressing prefixes not needed for data traffic. Transit-only networks that connect two routers are usually configured with routing IP addresses that are advertised in the Links State Advertisements (LSAs). However, these prefixes are not needed for data traffic. Prefixes can be suppressed for an OSPF process, an OSPF area, or for specific interfaces of a router. Prefix suppression is supported for OSPF and OSPFv3. **DHCP Duplicate MAC Session with Exclude VLAN Option** DHCP duplicate MAC session feature is now enhanced with an option to exclude inner and outer VLANs from the client key. Only MAC and interface are used to form the client key. A new exclude-vlan option is now available to the duplicate-mac-allowed command for excluding the VLANs. **Named Tunnel** The named tunnel feature lets you name the TE tunnels in the network with unique tunnel IDs to be able to manage the network with more ease. This feature allows you to provision TE tunnels using names. **Layer 3 Multicast Bundle Sub-Interface Load Balancing** The Layer 3 (L3) multicast bundle sub-interface load balancing feature allows you statically configure hash values to gain more control for bandwidth allocation (to make sure there is no oversubscription) and QoS (Quality of Service).
BGP	**BGP Optimal Route Reflector** BGP-ORR (optimal route reflector) enables virtual route reflector (vRR) to calculate the best path from a route reflector (RR) client's point of view. **BGP Neighbor Capability Suppression** A BGP speaker can learn about BGP extensions that are supported by a peer by using the capabilities negotiation feature. Capabilities negotiation allows BGP to use only the set of features supported by both BGP peers on a link. The neighbor capability suppression feature will turn off neighbor capabilities negotiation during Open message exchange. This is required for interoperability with very old customer premises equipment devices that do not understand Capabilities option. **Border Gateway Protocol Link-State** Border gateway protocol link-state (BGP LS) is an Address Family Identifier (AFI) and Sub-address Family Identifier (SAFI) defined to carry interior gateway protocol (IGP) link-state database through BGP. BGP LS delivers network topology information to topology servers and Application Layer Traffic Optimization (ALTO) servers. BGP LS supports IS-IS and OSPFv2.
IPv6	**IPv6 Support for RFC 4191 and RFC 6106** **RFC 4191:** Using the Neighbor Discovery (ND) Router Advertisement (RA) messages, a host has a choice to select the default router based on the "router-preference" option. **RFC 6106:** You can configure RA-based DNS in networks where an IPv6 host's address is auto-configured through IPv6 stateless address auto configuration and where there is either no DHCP IPv6 infrastructure or some hosts do not have a DHCP IPv6 client. IPv6 RA options also allow IPv6 routers to advertise a list of DNS recursive server addresses and a DNS search list to IPv6 hosts.

Feature	Description
EVPN	**EVPN ESI Multipath** With Ethernet VPN (EVPN) Ethernet Segment Identifier (ESI) Multipath feature, it is possible to support redundant are active-active paths between Top of the Rack (TORs) and the Data Center Interconnect (DCI) node. One of primary benefit is to allow load-sharing traffic across the 2 paths from the Dual homed TOR resulting in better utilization of network resources while providing redundant connectivity within the data center. With this feature, the ASR9000 acting as DCI is able to discover ESI multi paths using EVPN. **EVPN VXLAN Layer 2 Data Center Interconnect Gateway** The Cisco ASR 9000 Series Router serve as a Data Center Interconnect (DCI) Layer 2 gateway to provide Layer 2 connectivity between EVPN-VXLAN based data centers over a MPLS based L2VPN network. The data centers are connected through the intermediate service provider network. This feature provides redundancy, resiliency, and ease of provisioning.
Management	**OpFlex Support** OpFlex is an open and extensible policy protocol used for transferring the policy information between a network policy controller such as the Cisco Application Policy Infrastructure Controller (APIC) and network element such as routers that are configured as Data Center Interconnect (DCI) gateway. With OPFLEX, the ASR9000 acting as a DCI communicates with Cisco APIC controller and implement its policies. The policies are distributed using the Cisco Application Centric Infrastructure (ACI) infrastructure within the fabric to the spine nodes. The spine nodes send the policies to the DCI gateway through the OpFlex framework. Policies configure the DCI service for a given tenant on the DCI gateway.
MACsec	**MACsec Technology as a Service** MACsec can now be deployed as a service for L2 and L3 VPN sessions over a provider network. This provides a mechanism to provide encryption/decryption service on the Provider-Edge router for selected traffic across the WAN.
Consumption model enhancements	ASR 9000 consumption model is expanded to now include one new line card: - A9K-MOD400-CM This line card requires a minimum of 100G of foundation SW licenses (e.g., 20 x 10G right to use licenses), which provide a license for the transport protocol as well as port enablement. In addition, advanced software licenses can be added on a per 10G basis for protocols such as Ethernet OAM or to convert a "TR" port into "SE" with the hierarchical QoS license.
DHCP enhancements	**Rich DHCP Option on RADIUS Vendor Specifc Attributes** Rich DHCP option is an enhancement to DHCPv4 server profile whereby BNG provides per subscriber-based DHCP options to the end user through DHCP protocol messages. These options are the ones that are retrieved by BNG as Cisco- attribute-value pairs (AVPs) from the AAA Server. Each AVP carries a generic DHCPv4 option. This feature helps in configuring various DHCP IPv4 options on a per-subscriber basis. **DHCP Options Support for BNG DHCPv6 Proxy Mode** This is a DHCP enhancement where BNG DHCPv6 proxy supports addition of PPPoE attributes like Remote-Id, Circuit-Id and Username as DHCPv6 options in the Relay-forward message sent to the external DHCPv6 server. The DHCPv6 options are sent as Remote-Id, Interface-Id and Relay-Agent-Subscriber-Id respectively. The MAC-address can also be included as Link-layer Address option in Relay-forward message. These fields can then be used by the external DHCPv6 server while performing IPv6 prefix allocation for the end user. This feature helps in identifying subscribers based on the Interface-Id and Remote-Id attributes in PPPoE. **DHCP Option 60 Filtering** DHCP option 60 filtering in BNG provides support to either block or permit the subscribers or both, based on the DHCPv4 option 60 (Vendor-Id or Class-Id) field. This feature provides administrator the flexibility to drop illegal clients (with blocked listed Vendor-Id) at an early stage of DHCP session handling.
L2VPN	**L2TPv3 over IPv4** Layer 2 Tunneling Protocol version 3 (L2TPv3) over IPv4 provides a dynamic mechanism for tunneling Layer 2 (L2) circuits across a packet-oriented data network, with multiple attachment circuits multiplexed over a single pair of IP address endpoints, using the L2TPv3 session ID as a circuit discriminator. **Service Path Preference for L2VPN** Service Path Preference (SPP) for L2VPN enables L2VPN services to control which transport path to follow. Service provider have the flexibility to direct and assign L2VPN services to specific Traffic Engineering (TE) paths. With this feature, Services are given the ability to control what path in the network to follow. SPP uses powerful control plane policies providing much flexibility of configuration. SPP is supported for per-service (VFI) path selection for VPLS with BGP AD, and EVI for PBB-EVPN. **L2VPN Route Policy** L2VPN route-policy feature enables the export community configuration for L2VPN VPWS and L2VPN VPLS with BGP auto discovery. BGP executes the route-policy. This functionality is similar to the route-policy support under BGP sub mode for L3VPN services.
Seamless Bidirectional Forwarding Detection	Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines. BFD allows a single mechanism to be used for failure detection over any media and at any protocol layer, with a wide range of detection times and overhead. In BFD, each end of the connection maintains a BFD state and transmits packets periodically over a forwarding path. Seamless BFD (SBFD) is unidirectional, resulting in faster session activation. The BFD state and client context is maintained on the head-end (initiator) only. The tail-end (reflector) validates the BFD packet and responds, so there's no need to maintain the BFD state on the tail-end.

Feature	Description
Timing & Synchronization	**IEEE 1588 Precision Time Protocol (PTP) Telecom Profile G.8275.1** This fulfills the time-of-day and phase synchronization requirements in telecom networks with all network devices participating in the PTP protocol. G.8275.1 profile network with SyncE provides better frequency stability for the time-of-day and phase synchronization. **SyncE Support on Cisco IOS XR Software 64 bit** SyncE is now supported on Cisco IOS XR Software 64 bit for the line cards, A9K-8X100GE-SE/TR and A9K-4X100GE-SE/TR, on 100G (LAN and OTN transport modes) and 10G (LAN, WAN, and OTN transport modes) interfaces.
nV Satellite	On Cisco NCS500x satellites, QoS offload on access ports and non-bundle ICLs, Fabric CFM for both physical and bundle ICLs and dual head topologies are supported in this release. Similarly, fabric CFM on bundle ICLs is also supported for Cisco ASR 9000v satellites. **Native Image and SMU Push Support for Cisco NCS 500x nV satellites** Cisco ASR 9000 host supports the capability to push native Cisco NCS 500x images and SMU fixes from the host similar to nV satellite pie image upgrades from Cisco IOS XR Software Release 6.1.2 onwards. This provides the flexibility of managing the software images and pies on the satellite and also offers the zero touch provisioning model of nV satellites. The commands that are run on the host for addition and activation of both upgrade images and mandatory SMUs allows a fast turnaround time for any critical fixes on Cisco NCS 500x satellite. **Support of 10x10G ICLs on Cisco NCS500x satellites** A maximum of 10x10G ICL ports can be connected from the Cisco NCS 500x satellite to each of the Cisco ASR 9000 host in a Layer 1 Hub and Spoke topology (both single and dual head) using this feature. Along with the 10G ICL ports, the 4x100 GigE ICL ports can also be used with each of the hosts. The 10G ICLs have to be configured using the configurable fabric port feature. The 10x10G ICL links can be configured as members of a Bundle ICL or Physical ICL. If they are used as members of a Bundle ICL, then members must be distributed across NPs or line cards to achieve redundancy and overcome access port scale constraints.

Ordering Information

Table 3 lists ordering information for Cisco IOS XR Software Release 6.1.2 for Cisco ASR 9000 Series routers. When future rebuilds of Cisco IOS XR Software Release 6.1 are available, the latest release is automatically shipped when this product is ordered.

Table 3. Ordering Information for Cisco IOS XR Software and IOS XRv Software Release 6.1.2

Part Number	Product Name
XR-A9K-X64-06.1	Cisco IOS XR 64-bit IP/MPLS Core Software
XR-A9K-X64K9-06.1	Cisco IOS XR 64-bit IP/MPLS Core Software 3DES
XR-A9K-PX-06.01	Cisco IOS XR IP/MPLS Core Software
XR-A9K-PXK9-06.01	Cisco IOS XR IP/MPLS Core Software 3DES
R-XRV9000-601-RR	Cisco IOS XRV 9000 64-bit software. vRR profile
R-XRV9000-601-RRVG	Cisco IOS XRV 9000 64-bit software, vRR profile with VGA support
R-XRV9000-601	Cisco IOS XRV 9000 64-bit software, non-VRR profile
R-XRV9000-601-VG	Cisco IOS XRV 9000 64-bit software, non-vRR profile with VGA support

Cisco IOS XR Software Release 6.1.2 Lifecycle

The Cisco IOS XR Software release strategy is time-based, with a fixed release date and lifecycle, rather than being a feature-based release strategy with a variable release date. Table 4 lists the major milestones of Cisco IOS XR Software Release 6.1.2.

Table 4. Major Milestones for Cisco IOS XR Software Release 6.1.2

Milestone	Definition	Date
Availability date	The date that Cisco IOS XR Software Release 6.1.1 information is published on Cisco.com and becomes available to the general public.	August 31, 2016
End-of-life announcement date	The date when official end-of-life documents announcing the end of sale and end of life of Cisco IOS XR Software 6.0.1 (and later versions of 6.1.1) are distributed to the general public.	February 28, 2017
End-of-sale date	The last date to order Cisco IOS XR Software 6.1.1 through Cisco point-of-sale mechanisms. (The product is no longer for sale after this date.)	February 28, 2018
End of software maintenance (Standard Maintenance Release)	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. (After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.) Applies to Standard rebuilds 6.1.2 only. Refer to Cisco IOS XR Software Policy Guideline bulletin for more details (http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xr-software/product_bulletin_c25-478699.html).	August 31, 2018
End of software maintenance (Extended Maintenance Release)	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. (After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.) Applies to Standard rebuilds 6.1.3 only. Refer to Cisco IOS XR Software Policy Guideline bulletin for more details (http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xr-software/product_bulletin_c25-478699.html).	August 31, 2019
End of software maintenance for Product Security Incident Response Team (PSIRT)	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for PSIRTs through Software Maintenance Unit to Release 6.1. (Beyond this date, PSIRT bugs become candidates for following feature releases.)	August 31, 2020
Last date of support	The last date to receive applicable service and support for the product, as entitled by active service contracts or by warranty terms and conditions. (After this date, all support services for the product are unavailable, and the product becomes obsolete.)	February 28, 2023

For More Information

For more information regarding this release, visit:

- Cisco ASR 9000 Series Release Notes:
  http://www.cisco.com/c/en/us/support/routers/asr-9000-series-aggregation-services-routers/products-release-notes-list.html.

- Cisco IOS XRv Release Notes:
  http://www.cisco.com/c/en/us/td/docs/ios_xr_sw/ios_xrv/release/notes/xrv-rn.html.

- For official end-of-life and end-of-sale announcements for Cisco IOS XR Software, visit
  http://www.cisco.com/en/US/products/ps5845/prod_eol_notices_list.html or contact your local Cisco account representative.

- For additional information about the Cisco ASR 9000 Series or Cisco IOS XR Software, visit
  http://www.cisco.com/ or contact your local Cisco account representative.