Introduction to the Cisco ASR 9000 Series Aggregation Services Router

This chapter introduces the routers that support Cisco IOS XR software. It also introduces router concepts, features, and user interfaces.

Contents

- Supported Standalone System Configurations, page 1-1
- Cisco ASR 9000 Series Router Overview, page 1-3
- Management and Security, page 1-12
- Initial Router Configuration, page 1-14
- Router Management Interfaces, page 1-16
- Selecting and Identifying the Active RSP, page 1-17
- Connecting to the Router Through the Console Port, page 1-18
- Where to Go Next, page 1-22

Supported Standalone System Configurations

The Cisco IOS XR software runs on the following standalone systems:

- Cisco ASR 9000 Series Router 6-Slot Chassis
Supported Standalone System Configurations

Chapter 1  Introduction to the Cisco ASR 9000 Series Aggregation Services Router

Figure 1-1  6-Slot Chassis

- Cisco ASR 9000 Series Router 10-Slot Chassis

Figure 1-2  10-Slot Chassis

Each chassis type supports a capacity of up to 400 G per slot. The amount of this possible capacity, which is usable as consumable bandwidth, is dependent on the choice of line card (LC). Each chassis type also uses the same Route Switch Processors (RSPs) and LCs, which are interchangeable. In each chassis, two slots are designated for RSPs, whereas the remaining slots accommodate LCs that carry the traffic. The
RSPs interconnect the LCs for data plane and provide chassis management and control. Any LC can be used as a network-facing trunk card or a subscriber-facing card. It can also provide any other form of connectivity.

The router uses the following LCs:
- 4-port 10GE LC (A9K-4T-L, A9K-4T-E, A9K-4T-B)
- 8-port 10GE oversubscribed LC (A9K-8T/4-L, A9K-8T/4-E, A9K-8T/4-B)
- 8-port 10GE LC (A9K-8T-L, A9K-8T-E, A9K-8T-B)
- 16-port 10GE oversubscribed LC (A9K-16T/8-B)
- Cisco ASR 9000 Series SPA Interface Processor-700 (A9K-SIP-700)
- 24-Port 10-Gigabit Ethernet LC
- 2-Port 100-Gigabit Ethernet LC
- 20-Port Gigabit Ethernet Modular Port Adaptor
- 4-Port 10 Gigabit Ethernet Modular Port Adaptor
- 2-Port 10 Gigabit Ethernet Modular Port Adaptor
- 1-Port and 3-Port Clear Channel OC-3 ATM SPA
- 1-Port Clear Channel OC-12 ATM SPA

The backplane Gigabit Ethernet links, one to each RSP card, are used primarily for control plane functions such as application image download, system configuration data from the IOS XR software, statistics gathering, and line card power-up and reset control.

There are two types of image files: -P PIE files and -PX PIE files. The -P PIE files are used on Cisco ASR 9000 Series Aggregation Services Routers with RSP route switch processors while the -PX PIE files are used on Cisco ASR 9000 Series Aggregation Services Routers with RSP-400 route switch processors.

Cisco ASR 9000 Series Router Overview

The Cisco ASR 9000 Series Router serves multiple functions. It can serve as:
- a multilayer Ethernet switching and aggregation platform
- a label edge router (LER) that sits at the edge of a Multiprotocol Label Switching (MPLS) network
- a Multi-Service Edge (MSE) router connecting various access media technologies

The router has links that extend outside the MPLS network. It provides access and aggregation services for enterprise and service providers.

Features and Capabilities

The router is a scalable carrier-class distributed forwarding router, which is designed for redundancy, high security and availability, packaging, power, and other requirements needed by service providers.
The router aggregates triplie play Multi-service edge and Ethernet service traffic aggregating these services to 10 Gigabit Ethernet IP, MPLS edge, or core. It support Ethernet, serial (including MLPPP), frame relay and POS interface on the access side and Ethernet or POS interfaces on the core side.

The following sections describe the features and capabilities in detail:

- Cisco IOS XR Software, page 1-4
- Flexible Ethernet, page 1-7
- L2VPN, page 1-7
- Multicast, page 1-8
- OAM, page 1-8
- Layer 3 Routing, page 1-9
- MPLS VPN, page 1-10
- QoS, page 1-10
- MPLS TE, page 1-11

Cisco IOS XR Software

The router runs Cisco IOS XR Software, which offers the following:

- Rich Networking Feature Set—Cisco IOS XR Software represents a continuation of the Cisco networking leadership in helping customers realize the power of their networks and the Internet. It provides unprecedented routing-system scalability, high availability, service isolation, and manageability to meet the mission-critical requirements of next-generation networks.
- Operating system infrastructure protection—Cisco IOS XR Software provides a microkernel architecture that forces all but the most critical functions, such as memory management and thread distribution, outside of the kernel, thereby preventing failures in applications, file systems, and even device drivers from causing widespread service disruption.
- Process and thread protection—Each process, even individual process thread, is executed in its own protected memory space, and communications between processes are accomplished through well-defined, secure, and version-controlled application programming interfaces (APIs), significantly minimizing the effect that any process failure can have on other processes.
- Cisco In-Service Software Upgrade (ISSU)—Cisco IOS XR Software modularity sustains system availability during installation of a software upgrade. ISSUs or hitless software upgrades (HSUs) allow you to upgrade most Cisco router software features without affecting deployed services. You can target particular system components for upgrades based on software packages or composites that group selected features. Cisco preconfigures and tests these packages and composites to help ensure system compatibility.
- Process restart—You can restart critical control-plane processes both manually and automatically in response to a process failure versus restarting the entire operating system. This feature supports the Cisco IOS XR Software goal of continuous system availability and allows for quick recovery from process or protocol failures with minimal disruption to customers or traffic.
- State checkpoint—You can maintain a memory and critical operating state across process restarts to sustain routing adjacencies and signaling state during a Route Switch Processor (RSP) switchover.
- Ethernet virtual connections (EVCs)—Ethernet services are supported using individual EVCs to carry traffic belonging to a specific service type or end user through the network. You can use EVC-based services in conjunction with MPLS-based L2VPNs and native IEEE bridging deployments.
Cisco ASR 9000 Series Aggregation Services Router

Chapter 1       Introduction to the Cisco ASR 9000 Series Aggregation Services Router

Cisco ASR 9000 Series Router Overview

• Flexible VLAN classification—VLAN classification into Ethernet flow points (EFPs) includes single-tagged VLANs, double-tagged VLANs (QinQ and IEEE 802.1ad), contiguous VLAN ranges, and noncontiguous VLAN lists.

• IEEE Bridging—Software supports native bridging based on IEEE 802.1Q, IEEE 802.1ad, IEEE 802.1ah provider backbone bridges (PBB) and QinQ VLAN encapsulation mechanisms on the router.

• IEEE 802.1s Multiple Spanning Tree (MST)—MST extends the IEEE 802.1w Rapid Spanning Tree Protocol (MSTP) to multiple spanning trees, providing rapid convergence and load balancing.

• MST Access Gateway—This feature provides a resilient, fast-convergence mechanism for aggregating and connecting to Ethernet-based access rings.

• Virtual Private LAN Services (VPLS)—VPLS is a class of VPN that supports the connection of multiple sites in a single, bridged domain over a managed IP/MPLS network. It presents an Ethernet interface to customers, simplifying the LAN and WAN boundary for service providers and customers, and enabling rapid and flexible service provisioning because the service bandwidth is not tied to the physical interface. All services in a VPLS appear to be on the same LAN, regardless of location.

• Hierarchical VPLS (H-VPLS)—H-VPLS provides a level of hierarchy at the edge of the VPLS network for increased scale. QinQ access and H-VPLS pseudowire access options are supported.

• Virtual Private WAN Services/Ethernet over MPLS (VPWS/EoMPLS)—EoMPLS transports Ethernet frames across an MPLS core using pseudowires. Individual EFPs or an entire port can be transported over the MPLS backbone using pseudowires to an egress interface or subinterface.

• Pseudowire redundancy—Pseudowire redundancy supports the definition of a backup pseudowire to protect a primary pseudowire that fails.

• Multisegment pseudowire stitching—Multisegment pseudowire stitching is a method for interworking two pseudowires together to form a cross-connect relationship.

• IPv4 Multicast—IPv4 Multicast supports Internet Group Management Protocol Versions 2 and 3 (IGMPv2/v3), Protocol Independent Multicast Source Specific Multicast (SSM) and Sparse Mode (SM), Multicast Source Discovery Protocol (MSDP), and Anycast Rendezvous Point (RP).

• IGMP v2/v3 Snooping—This Layer 2 mechanism efficiently tracks multicast membership on an L2VPN network. Individual IGMP joins are snooped at the VLAN level or pseudowire level, and then it summarizes the results into a single upstream join message. In residential broadband deployments, this feature enables the network to send only channels that are being watched to the downstream users.

• NxDS0—This feature allows channelization of the Cisco 2-Port Channelized OC-12/DS0 SPA to interface speeds as low as 56 kbit. To add bandwidth, you can combine channel groups/timeslots. For more information on NxDS0, see Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

• Virtual Router Redundancy Protocol (VRRP) over IPv6—This feature provides support to virtual IPv6 addresses. VRRP Version 3 is implemented for both IPv4 and IPv6. This feature also includes VRRP support for IPv6 Virtual Routing and Forwarding (VRF) and Bidirectional Forwarding Detection (BFD). For more information on VRRP over IPv6, see the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

• Lawful Intercept IPv4—Lawful intercept is the process by which law enforcement agencies conduct electronic surveillance of circuit-mode and packet-mode communications, authorized by either a judicial order or an administrative order. Service providers worldwide are legally required to assist law enforcement agencies in conducting electronic surveillance in both circuit-switched and packet-mode networks. For more information on Lawful Intercept IPv4, see the Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide.
Ethernet-Local Management Interface (E-LMI)—E-LMI is an asymmetric protocol that runs on the PE-to-CE link or the User-Network Interface (UNI). The user-facing Provider Edge (uPE) device uses E-LMI to communicate the connectivity status (EVC status) and configuration parameters of the Ethernet services available on the UNI of the CE device. For more information on configuring E-LMI, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Multigigabit Service Control Platform (MGSCP)—The MGSCP solution uses EtherChannel (EC) and the Link Aggregation Control Protocol (LACP) 802.3ad to enable the task of scaling the SCE platform by sending the traffic to an EC. EC load balancing is used to distribute the traffic over several SCE platforms. For more information on MGSCP, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Integrated Routing and Bridging (IRB) Interoperability Support on ASR 9000 SIP-700—This feature provides IRB interoperability support between SIP-700 and Ethernet line cards. For more information on IRB interoperability support, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

IPv6 Access Services: Dynamic Host Configuration Protocol (DHCP) Relay Agent—RFC 3315 defines the DHCP relay agent that resides on a client's link and relays messages between the client and the server. This agent allows a DHCP client to send a message to a DHCP server that is not connected to the same link. For more information on the DHCP Relay Agent, see the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

Integrated Service Module (ISM)—This feature is used for video integration and other services, such as content streaming on the ASR9000-SIM-100 platform. For more information on installing the ISM line cards, see the Cisco ASR 9000 Series Aggregation Services Router ISM Line Card Installation Guide.

IEEE 802.1ab Link Layer Discovery Protocol (LLDP)—This feature enables the task of discovering the network topology in a standardized way using standard management tools, such as SNMP. The LLDP is initially deployed in Ethernet-based enterprise switching networks, which can also be used over other media types, such as Token Ring and FDDI. For more information on configuring LLDP, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

High Availability for Lawful Intercept—This feature provides operational continuity of the TAP flows and provisioned MD tables to reduce loss of information due to route processor fail over (RPFO). For more information on high availability for lawful intercept, see the Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide.

Bidirectional Forwarding (BFD) on Multiple Hops—This feature provides sub-second forwarding failure detection for a destination more than one hop, and up to 255 hops, away. BFD multihop is supported on all currently supported media-type for BFD singlehop. For more information on how to configure BFD sessions, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Circuit Emulation over Packet Switched Network (CEoP)—This is a way to carry TDM circuits over packet switched network. For more information see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Link Bundling - PoS—This feature supports link bundling on the PoS interfaces. For more information on how to configure the PoS link bundles, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Unidirectional Link Detection (UDLD) on ASR 9000—This feature supports link fault detection on the physical Ethernet interfaces, which uses a defined link fault message to signal link faults to a remote host. For more information, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.
Chapter 1  Introduction to the Cisco ASR 9000 Series Aggregation Services Router

Cisco ASR 9000 Series Router Overview

- Generic Routing Encapsulation (GRE) Support for L3VPN—GRE is a tunneling protocol that can encapsulate many types of packets to enable data transmission using a tunnel. For more information on GRE, see the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

- Multiple Group Optimization (MGO) for HSRP—This feature provides a solution for reducing control traffic in a deployment consisting of many subinterfaces. For more information on how to reduce the traffic using the MGO, see the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

- MPLS Transport Profile (MPLS-TP)—This feature enables you to create tunnels that provide the transport network service layer over which IP and MPLS traffic traverse. For more information, see the Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide.

- Broadband Network Gateway (BNG)—This feature provides a number of capabilities that helps to improve the service provider's ability to control the subscriber's services and to simplify overall network operations. For more information on how to implement the BNG features, see the Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide.

- Video Monitoring Unicast—This feature plays a significant role in improving the video quality and enhancing the quality of experience. For more information on how video monitoring is implemented on the routers, see the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

Flexible Ethernet

The router uses Ethernet as its transport mechanism, which offers the following:

- Ethernet virtual connections (EVCs)—Ethernet services are supported using individual EVCs to carry traffic belonging to a specific service type or end user through the network. You can use EVC-based services in conjunction with MPLS-based L2VPNs and native IEEE bridging deployments.

- Flexible VLAN classification—VLAN classification into EFPs includes single-tagged VLANs, double-tagged VLANs (QinQ and IEEE 802.1ad), contiguous VLAN ranges, and noncontiguous VLAN lists.

- IEEE Bridging—The software supports native bridging based on IEEE 802.1Q, IEEE 802.1ad, and QinQ VLAN encapsulation mechanisms on the router.

- IEEE 802.1s Multiple Spanning Tree (MST)—MST extends the MSTP to multiple spanning trees, providing rapid convergence and load balancing.

- MST Access Gateway—This feature provides a resilient, fast-convergence mechanism for aggregating and connecting to Ethernet-based access rings.

L2VPN

The router uses L2VPNs, which offers the following:

- Virtual Private LAN Services (VPLS)—VPLS is a class of VPN that supports the connection of multiple sites in a single, bridged domain over a managed IP/MPLS network. It presents an Ethernet interface to customers, simplifying the LAN and WAN boundary for service providers and customers, and enabling rapid and flexible service provisioning because the service bandwidth is not tied to the physical interface. All services in a VPLS appear to be on the same LAN, regardless of location.
Cisco ASR 9000 Series Router Overview

- Hierarchical VPLS (H-VPLS)—H-VPLS provides a level of hierarchy at the edge of the VPLS network for increased scale. QinQ access and H-VPLS pseudowire access options are supported.
- Virtual Private WAN Services/Ethernet over MPLS (VPWS/EoMPLS)—EoMPLS transports Ethernet frames across an MPLS core using pseudowires. Individual EFPs or an entire port can be transported over the MPLS backbone using pseudowires to an egress interface or subinterface.
- Pseudowire redundancy—Pseudowire redundancy supports the definition of a backup pseudowire to protect a primary pseudowire that fails.
- Multisegment pseudowire stitching—This is a method used to interwork two pseudowires together to form a cross-connect relationship.
- G.8032 Support—This feature implements the Automatic Protection Switching (APS) protocol and protection switching mechanisms for Ethernet layer ring topologies. For more information on G.8032 support, see the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.
- Multiple Spanning Tree Access Gateway (MSTAG) Edge Mode—Using this feature, you can configure the MSTAG in such a way that the gateway devices have the best path to the best possible Multiple Spanning Tree Protocol (MSTP) root node. For more information on MSTAG Edge mode, see the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.
- Virtual Private LAN Services (VPLS) Support on ASR 9000 SIP-700—VPLS is a mechanism for transporting Ethernet traffic across multiple sites that belong to the same L2 broadcast domain. This feature builds a point-to-point connection to interconnect two customer sites. For more information on VPLS support, see the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

Multicast

- IPv4 Multicast—IPv4 Multicast supports Internet Group Management Protocol Versions 2 and 3 (IGMPv2/v3), Protocol Independent Multicast Source Specific Multicast (SSM) and Sparse Mode (SM), Multicast Source Discovery Protocol (MSDP), and Anycast Rendezvous Point (RP).
- IGMP v2/v3 Snooping—This Layer 2 mechanism efficiently tracks multicast membership on an L2VPN network. Individual IGMP joins are snooped at the VLAN level or pseudowire level, and then it summarizes the results into a single upstream join message. In residential broadband deployments, this feature enables the network to send only channels that are being watched to the downstream users.
- Multicast VPN Extranet Support—This feature enables service providers to distribute IP multicast content originated from one enterprise site to other enterprise sites. This feature enables service providers to offer the next generation of flexible extranet services, helping to enable business partnerships between different enterprise VPN customers.

OAM

- E-OAM (IEEE 802.3ah)—Ethernet link layer OAM is a vital component of EOAM that provides physical-link OAM to monitor link health and assist in fault isolation. Along with IEEE 802.1ag, Ethernet link layer OAM can be used to assist in rapid link-failure detection and signaling to remote end nodes of a local failure.
E-OAM (IEEE 802.1ag)—Ethernet Connectivity Fault Management is a subset of EOAM that provides numerous mechanisms and procedures that allow discovery and verification of the path through IEEE 802.1 bridges and LANs.

MPLS OAM—This protocol supports label-switched-path (LSP) ping, LSP TraceRoute, and virtual circuit connectivity verification (VCCV).

Layer 3 Routing

The router runs Cisco IOS XR Software, which supports Layer 3 routing and a range of IPv4 services and routing protocols, including the following:


- Open Shortest Path First (OSPF)—OSPF is an IGP developed by the OSPF working group of the Internet Engineering Task Force (IETF). For more information on OSPF, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

- Static Routing—Static routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. For more information on static routing, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

- IPv4 Multicast—IPv4 Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. For more information on IPv4 Multicast, see Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide.

- Routing Policy Language (RPL)—RPL provides a single, straightforward language in which all routing policy needs can be expressed. For more information on RPL, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

- Hot Standby Router Protocol (HSRP)—HSRP is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. For more information on HSRP, see Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

- Virtual Router Redundancy Protocol (VRRP)—VRRP allows for transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router. For more information on VRRP, see Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

- Border Gateway Protocol (BGP) Add Path—This feature enables a BGP speaker to send multiple paths for a prefix. For more information on BGP Add Path, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

- Selective VRF Download (SVD)—This feature allows to download only those prefixes and labels to a line card that are actively required to forward traffic through that line card. For more information on SVD, see the Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

- Route and Label Consistency Checker (RCC and LCC)—The RCC and LCC is used to verify the consistency between control plane and data plane route and label programming in IOS XR Software. For more information on how to use the RCC and LCC, see the Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.
• System-Wide Route and Label Prioritization—This feature provides faster and more consistent Interior Gateway Protocol (IGP) convergence due to router or network events. For more information on how to prioritize and download the critical routes and labels, see the Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

**MPLS VPN**

The router supports MPLS VPN, which offers the following:

• MPLS L3VPN—This IP VPN feature for MPLS allows a Cisco IOS Software or Cisco IOS XR software network to deploy scalable IPv4 Layer 3 VPN backbone services. An IP VPN is the foundation that companies use for deploying or administering value-added services, including applications and data hosting network commerce and telephony services, to business customers.

• Carrier Supporting Carrier (CSC)—CSC allows an MPLS VPN service provider to connect geographically isolated sites using another backbone service provider and still maintain a private address space for its customer VPNs. It is implemented as defined by IETF RFC 4364.

• Inter-AS—is a peer-to-peer type model that allows extension of VPNs through multiple provider or multi-domain networks. This lets service providers peer up with one another to offer end-to-end VPN connectivity over extended geographical locations. An MPLS VPN Inter-AS allows:
  - VPN to cross more than one service provider backbone.
  - VPN to exist in different areas.
  - confederations to optimize Internal Border Gateway Protocol (iBGP) meshing.

• MPLS VPN OSPFv3 PE-CE—This feature provides support for the Open Shortest Path First version 3 (OSPFv3) routing protocol between the provider edge-to-customer edge (PE-CE) router over IPv6 L3VPN. For more information on MPLS VPN, see the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

**QoS**

The router supports many types of quality of service (QoS), which offers the following:

• QoS—Comprehensive QoS support with up to 3 million queues, Class-Based Weighted Fair Queuing (CBWFQ) based on a three-parameter scheduler, Weighted Random Early Detection (WRED), two-level strict priority scheduling with priority propagation, and 2-rate, 3-color (2R3C) Policing are all supported.

• Cisco IOS XR Software—This software supports a rich variety of QoS mechanisms, including policing, marking, queuing, dropping, and shaping. In addition, the operating systems support Modular QoS CLI (MQC). Modular CLI is used to configure various QoS features on various Cisco platforms.

• H-QoS—Is supported on both the SIP based interfaces and the Ethernet interfaces. For EVCs four-level H-QoS support is provided with the following hierarchy levels: port, group of EFPs, EFP, and class of service. This level of support allows for per-service and per-end user QoS granularity. For information about three-level QoS for SIP based interfaces, see Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide.

• Four-level H-QoS support is provided for EVCs with the following hierarchy levels: port, group of EFPs, EFP, and class of service. This level of support allows for per-service and per-end user QoS granularity. H-QOS support is also provided on SIP based interfaces.
Chapter 1      Introduction to the Cisco ASR 9000 Series Aggregation Services Router

Cisco ASR 9000 Series Router Overview

- QoS Policy Propagation Using Border Gateway Protocol (QPPB)—QPPB allows BGP policy set in one location of the network to be propagated using BGP to other parts of the network, where appropriate QoS policies can be created. For more information on QPPB, see the Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide.

MPLS TE

The router supports MPLS Traffic Engineering (TE), which offers the following:

- MPLS—Cisco IOS XR Software supports MPLS protocols such as Traffic Engineering/Fast Reroute (TE-FRR), Resource Reservation Protocol (RSVP), Label Distribution Protocol (LDP), and Targeted Label Distribution Protocol (T-LDP).
- MPLS TE Preferred Path—Preferred tunnel path functions let you map pseudowires to specific TE tunnels. Attachment circuits are cross-connected to specific MPLS TE tunnel interfaces instead of remote provider-edge router IP addresses (reachable using IGP or LDP).
- Ignore Intermediate System-to-Intermediate System (IS-IS) Overload Bit Avoidance—This feature allows network administrators to prevent a RSVP-TE Label Switched Path (LSP) from being disabled when a router in that path has its Intermediate System-to-Intermediate System (IS-IS) overload bit set. For more information on IS-IS overload bit avoidance, see the Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide.
- Label Switched Multicast (LSM) Point-to-Multipoint (P2MP) Traffic Engineering (TE)—LSM is a solution framework providing multicast services over a customer’s MPLS or GMPLS backbone network. This feature uses the extensions to RSVP-TE to build P2MP trees. The data plane provides support for the MPLS replications. For more information on LSM, see the Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide.
- Soft-Preemption—Soft preemption is an extension to the RSVP-TE protocol to minimize or eliminate the traffic disruption over the preempted Label Switched Paths (LSP). For more information on how to achieve zero traffic loss, see the Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide.
- Path-Option Attributes—The path option attributes are configurable through a template configuration. This template, named attribute-set, is configured globally in the MPLS traffic-engineering mode. For more information on how to implement path option attributes, see the Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide.

High Availability

The router is intended for use in Service Provider and Enterprise networks that require high availability. It is designed to provide high MTBF (Mean Time Between Failures) and low MTTR (Mean Time To Resolve) rates. This minimizes outages and maximizes availability. The router achieves this using the following:

- Component redundancy
  - Duplex power supplies
  - Cooling systems
- Fault detection
- Management features
- High availability features
– Non-stop forwarding (NSF)—Cisco IOS XR Software supports forwarding without traffic loss during a brief outage of the control plane through signaling and routing protocol implementations for graceful restart extensions as standardized by the IETF. NSF requires neighboring nodes to be NSF-aware.
– Process restartability
– Stateful switchovers
– MPLS TE FRR
– Bidirectional Forwarding Detection (BFD)
– Standard IEEE 802.3ad link aggregation bundles

**Management and Security**

In addition to the following management and security features, the router has administrative options, such as assigning Task IDs, that control who can perform router tasks.

**Manageability**

- Cisco IOS XR Software manageability—This feature provides industry-standard management interfaces, including a modular CLI, SNMP, and native XML interfaces.
- Command-Line Interface (CLI)—CLI is a user interface for monitoring and maintaining the router and also for configuring basic router features.
- Simple Network Management Protocol (SNMP)—SNMP is an application-layer protocol that facilitates management information exchange between network devices.
- Trivial File Transfer Protocol (TFTP)—TFTP allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
- Network Time Protocol (NTP)—NTP synchronizes timekeeping among a set of distributed time servers.
- Cisco Active Network Abstraction (ANA)—Cisco ANA is a flexible, vendor-neutral network resource-management solution for a multitechnology, multiservice network environment. Operating between the network and the operations-support-system (OSS) layer, Cisco ANA aggregates virtual
network elements (VNEs) into a software-based virtual network, much as real network elements create the real-world network. Cisco ANA dynamically discovers network components and tracks the status of network elements in near real time. Cisco ANA offers service providers:

- Simplified integration of OSS applications with network information
- Flexible common infrastructure for managing network resources
- Consistent procedures and interfaces for all network elements

Security

- Cisco IOS XR Software—Provides comprehensive network security features as follows:
  - ACLs
  - Control-plane protection
  - Routing authentications
  - Authentication, Authorization, and Accounting (AAA)
  - TACACS+
  - Remote Authentication Dial In User Service (RADIUS)
  - IP Security (IPSec)
  - Secure Shell (SSH) Protocol
  - SNMPv3
  - Routing Policy Language (RPL)
- Layer 2 ACLs—Filters packets under an EVC based on MAC addresses.
- Layer 3 ACLs—Matches ACLs by IPv4 protocol packet attributes.
- Security—Supported features include:
  - Standard IEEE 802.1ad Layer 2 Control Protocol (L2CP) and bridge-protocol-data-unit (BPDU) filtering
  - MAC limiting per EFP or bridge domain
  - Unicast, multicast, and broadcast storm control blocking on any interface or port
  - Unknown Unicast Flood Blocking (UUFB)
  - Dynamic Host Configuration Protocol (DHCP) Snooping
  - Unicast Reverse Path Forwarding (URPF)
  - Control-plane security
- Secure Shell (SSH)
- Control Plane Policing (CoPP)

Cisco ASR 9000 Series SPA Interface Processor-700

Cisco ASR 9000 Series SPA Interface Processor-700 is a Quantum Flow Processor (QFP)10-based engine with up to four SPA interfaces. It is primarily designed to support non-Ethernet media to complement the family of Ethernet line cards available on the ASR 9000. This LC provides the ability to support multiple legacy services, for example, TDM, Frame Relay, ATM etc.
It is a 20G QFP LC for rich, flexible, extensible IP based services. The key application areas of this LC are Multi-Service Edge and Mobile Aggregation deployments.

Powered by the incredibly potent Cisco Quantum Flow Processor, the Cisco ASR 9000 Series SPA Interface Processor 700 (A9K-SIP-700) uses proven hardware and software designs to accelerate introduction of new and varied physical layers and enable a lower total cost of ownership (TCO).

The 4-bay A9K-SIP-700 doubles the capacity of previous-generation offerings. It provides powerful hierarchical quality of service (H-QoS), high multidimensional scalability, and support for rich Layer 3 services and features. The Cisco Quantum Flow Processor is a fully integrated and programmable chipset designed to unify massive parallel processing, advanced memory management, security, and sophisticated QoS mechanisms with virtual service delivery and programmability.

The Cisco ASR 9000 Series enable operators to deploy any combination of Layer 2 and Layer 3 service applications at an industry-leading price-to-performance ratio. The Cisco ASR 9000 SIP-700 is designed to complement this ability by, over time, extending the same scalability and reliability to the realm of traditional transport media such as time-division multiplexing (TDM), Frame Relay, ATM, and Packet over Sonet (POS), thereby reducing capital expenditures (CapEx) and operating expenses (OpEx), as well as reducing the time required to develop and deploy new services. It also allows service providers to continue their deployed services, keeping those revenue streams open, while simultaneously migrating to the next-generation routing platform that opens up new channels of revenue.

By seamlessly integrating within the same chassis, the SIP-700 and Ethernet line cards provide true network and device convergence - a key design goal for the Cisco ASR 9000 Series of routers. The Cisco ASR 9000 SIP-700 only utilizes one line card slot within the Cisco ASR 9000 Series chassis, saving valuable line-card real estate. Fully integrated with the Cisco ASR 9000 Series synchronization circuitry, the Cisco ASR 9000 SIP-700 line cards provide standards-based line-interface functions for delivering and deriving transport-class network timing, enabling support of network-synchronized services and applications such as mobile backhaul and time-division multiplexing (TDM) migration.

For more information about the Cisco ASR 9000 Series SPA Interface Processor-700, see the Cisco ASR 9000 Series Aggregation Services Router SIP and SPA Hardware Installation Guide.

**Figure 1-3  Cisco ASR 9000 Series SPA Interface Processor-700**

---

**Initial Router Configuration**

The initial configuration of the Cisco ASR 9000 Series Router is determined automatically by the software when you boot the router; you do not need to set up any general configuration information. Also, there is no explicit configuration needed to make a particular RSP active. It becomes the active RSP when chosen automatically by the software upon boot.
Because there is only one RSP pair in this router, the primary RSP choices are RSP0 and RSP1. Typically, the slot with the lower number is the chosen primary RSP. If that RSP is not available, the software chooses the RSP in the other slot as the elected Route Process Controller, making it the primary RSP; the other RSP becomes standby RSP. During switchover, the active role migrates to the standby RSP.
Management Interfaces

Although there is no need to set up general router configuration information, you do need to configure management interfaces manually. Configure management ports on RSP0, RSP1, or both at the same time using:

- Telnet
- SSH (v1 and v2)
- Console Server

Router Management Interfaces

The router provides different router management interfaces, described in the following sections:

- Command-Line Interface, page 1-16
- Extensible Markup Language API, page 1-16
- Simple Network Management Protocol, page 1-17

Command-Line Interface

The CLI is the primary user interface for configuring, monitoring, and maintaining routers that run Cisco IOS XR software. The CLI allows you to directly and simply execute Cisco IOS XR commands. All procedures in this guide use CLI. Before you can use other router management interfaces, you must first use the CLI to install and configure those interfaces. Guidelines for using the CLI to configure the router are discussed in the following chapters:

- Configuring General Router Features
- Configuring Additional Router Features
- CLI Tips, Techniques, and Shortcuts

For more information on CLI procedures for other tasks, such as hardware interface and software protocol management tasks, see the Cisco IOS XR software documents listed in the “Related Documents” section on page x.

Extensible Markup Language API

The Extensible Markup Language (XML) application programming interface (API) is an XML interface used for rapid development of client applications and perl scripts to manage and monitor the router. Client applications can be used to configure the router or request status information from the router by encoding a request in XML API tags and sending it to the router. The router processes the request and sends the response to the client in the form of encoded XML API tags. The XML API supports readily available transport layers, including Telnet, SSH, and Secure Socket Layer (SSL) transport.

For more information on XML, see the Cisco IOS XR software documents listed in the “Related Documents” section on page x.
Simple Network Management Protocol

*Simple Network Management Protocol (SNMP)* is an application-layer protocol that facilitates the exchange of management information between network devices. By using SNMP-transported data (such as packets per second and network error rates), network administrators can manage network performance, find and solve network problems, and plan for network growth.

The Cisco IOS XR software supports SNMP v1, v2c, and v3. SNMP is part of a larger architecture called the Internet Network Management Framework (NMF), which is defined in Internet documents called RFCs. The SNMPv1 NMF is defined by RFCs 1155, 1157, and 1212, and the SNMPv2 NMF is defined by RFCs 1441 through 1452. For more information on SNMP v3, see RFC 2272 and 2273.

SNMP is a popular protocol for managing diverse commercial internetworks and those used in universities and research organizations. SNMP-related standardization activity continues even as vendors develop and release state-of-the-art, SNMP-based management applications. SNMP is a relatively simple protocol, yet its feature set is sufficiently powerful to handle the difficult problems presented in trying to manage the heterogeneous networks of today.

For more information on SNMP, see the Cisco IOS XR software documents listed in the “Related Documents” section on page x.

Selecting and Identifying the Active RSP

A designated shelf controller (DSC) is a role that is assigned to one route switch processor (RSP) card in each router.

**Note**

Throughout this guide, the term RSP is used to refer to the RSP cards supported on Cisco ASR 9000 Series Routers. If a feature or an issue applies to only one platform, the accompanying text specifies the platform. The active RSP card acts as DSC in the system.

Although each router can have two RSP cards, only one can serve as the active RSP and control the router. The active RSP provides system-wide administrative functions, including:

- User configuration using a terminal connection or network connection
- Distribution of software to each node in the router or system
- Coordination of software versioning and configurations for all nodes in the router or system
- Hardware inventory and environmental monitoring

The first step in setting up a new router is to select or identify the active RSP because the initial router configuration takes place through the active RSP. The following section describes how to select and identify the DSC on different routers:

- Selecting and Identifying the DSC on Cisco ASR 9000 Series Routers, page 1-17

Selecting and Identifying the DSC on Cisco ASR 9000 Series Routers

A Cisco ASR 9000 Series Router supports up to two RSPs. If only one RSP is installed, that RSP automatically becomes the active RSP. If two RSPs are installed, the default configuration selects RSP0 as the active RSP. To select RSP1 to become the active RSP for a new installation, install RSP1 first, apply power to the system, and wait for RSP1 to start up. When the Primary LED on the RSP1 front panel lights, RSP1 is operating as the active RSP, and you can install RSP0.
Connecting to the Router Through the Console Port

The active RSP can be identified by the green Primary LED on the faceplate of the card. The alphanumeric LED display on the active RSP displays ACTV. By default, the other RSP becomes the standby RSP, displays STBY on the alphanumeric display, and takes over if the active RSP fails.

**Note**
The active RSP acts as DSC in the Cisco ASR 9000 Series Router.

Connecting to the Router Through the Console Port

The first time you connect to a new router with Cisco IOS XR software, you must connect through the Console port. Although typical router configuration and management take place using an Ethernet port, you must configure the console port for your LAN before it can be used.

Because a new router has no name, IP address, or other credentials, use a terminal to connect through the Console port, setting the speed to 9600. The remote terminal setting has to match the 9600 value.

After you connect through the Console port, configure the management ports with their IP addresses. Then, you can use either SSH or Telnet to connect to the router.

**Note**
confreg 0x0 reverts to the default speed setting. If you change it from the default of 9600, you must reset it afterward.

*Figure 1-4* shows the RSP connections on the Cisco ASR 9000 Series Router.
Figure 1-4 Communication Ports on the RSP Card for a Cisco ASR 9000 Series Router

| Figure 1-4 Communication Ports on the RSP Card for a Cisco ASR 9000 Series Router |
|---|---|
| 1 | Management LAN Ports |
| 2 | Console Port and Auxiliary Port |
| 3 | Sync (BITS and J.211) ports |
| 4 | Alarm Out DB9 Connector |
| 5 | Compact Flash type I/II |
| 6 | Alarm Cutoff (ACO) and Lamp Test push buttons |
| 7 | Eight discrete LED indicators |
| 8 | LED Matrix display |

To connect to the router through the Console port, perform the following procedure.
SUMMARY STEPS

1. Power on the router.
2. Connect a terminal to the Console port.
3. Start the terminal emulation program.
4. Press Enter.
5. Log in to the router.
6. admin
7. show dsc
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** Power on the router. | Starts the router.  
  - This step is required only if the power is not on.  
  - For information on power installation and controls, see the hardware documentation listed in the “Conventions”. |
| **Step 2** Connect a terminal to the Console port. | Establishes a communications path to the router.  
  - During the initial setup, you can communicate with the router only through the Console port.  
  - Router Console port is designed for a serial cable connection to a terminal or a computer that is running a terminal emulation program.  
  - Terminal settings are:  
    - Bits per second: 9600  
    - Data bits: 8  
    - Parity: None  
    - Stop bit: 2  
    - Flow control: None  
  - For information on the cable requirements for the Console port, see the hardware documentation listed in the “Conventions”. |
| **Step 3** Start the terminal emulation program. | (Optional) Prepares a computer for router communications.  
  - Not required if you are connecting through a terminal.  
  - Terminals send keystrokes to, and receive characters, from another device. If you connect a computer to the Console port, you must use a terminal emulation program to communicate with the router. For instructions on using the terminal emulation program, see the documentation for that program. |
| **Step 4** Press Enter. | Initiates communication with the router.  
  - If no text or router prompt appears when you connect to the console port, press Enter to initiate communications.  
  - If no text appears when you press Enter, give the router more time to complete the initial boot procedure, then press Enter.  
  - If the prompt gets lost among display messages, press Enter again.  
  - The router displays the prompt: Username:
Where to Go Next

Configuring the Router Data Interfaces

After connecting to the router, configure the data interfaces manually. These are Gigabit Ethernet, 10-Gigabit Ethernet interfaces or the SPA based interfaces available on the SIP card. Because these interfaces are for data traffic only, not management traffic, you cannot use SSH or Telnet to an IP address that is part of the interfaces. For more information about configuring Gigabit Ethernet and 10-Gigabit Ethernet interfaces, see the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Where to Go Next

If you have logged into the router, you can perform the general router configuration as described in CLI Prompt.

If the router is prompting you to enter a root-system username, bring up the router. For more information, see Chapter 2, “Bringing Up Cisco IOS XR Software on the Router”.