Introducing the Cisco ASR 9000 Series Aggregation Services Router

This chapter introduces the Cisco ASR 9000 Series router that runs Cisco IOS XR Software. It also introduces router concepts, features, and user interfaces.

Contents

- Router Overview, page 1-1
- System Configurations, page 1-6
- Management and Security, page 1-8
- Initial Router Configuration, page 1-9
- Where to Go Next, page 1-13

Router Overview

The Cisco ASR 9000 Series router is a multilayer Ethernet switching and aggregation platform. It is also a label edge router (LER) that sits at the edge of a Multiprotocol Label Switching (MPLS) network. The router has links that extend outside the MPLS network. It provides access and aggregation services for enterprise and service providers.

Features and Capabilities

A scalable, carrier-class distributed forwarding router, the router is designed for the redundancy, high security and availability, packaging, power and other requirements needed by service providers.

The router aggregates triple play and Ethernet service traffic from Gigabit Ethernet devices, aggregating these services to 10 Gigabit Ethernet IP, MPLS edge, or core.

The following sections describe the features and capabilities in detail:

- Cisco IOS XR Software, page 1-2
- Flexible Ethernet, page 1-3
- L2VPN, page 1-4
Cisco IOS XR Software

The Cisco ASR 9000 Series router runs Cisco IOS XR Software, this offers the following:

- Modular software design: 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 threads—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 checkpointing: You can maintain a memory and critical operating state across process restarts in order 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.
Flexible Ethernet 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: 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 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 summarizes 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.

Flexible Ethernet

The router uses Ethernet as its transport mechanism, this 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 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: 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 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.

L2VPN

The Cisco ASR 9000 Series router uses L2VPNs, this 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.

• 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 EFs 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.

Multicast

The Cisco ASR 9000 Series router supports multicast, this offers the following:

• 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 summarizes 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.

OAM

The Cisco ASR 9000 Series router supports different types of operations, administration, and maintenance (OAM), this offers the following:

• 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 Cisco ASR 9000 Series router runs Cisco IOS XR Software which supports Layer 3 routing and a range of IPv4 services and routing protocols, including the following:

- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
- static routing
- IPv4 Multicast
- Routing Policy Language (RPL)
- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)

MPLS VPN

The Cisco ASR 9000 Series router supports MPLS VPN, this offers the following:

- MPLS L3VPN: The 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 a 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.

QoS

The Cisco ASR 9000 Series router supports many types of quality of service (QoS), this 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. Additionally, the operating systems support Modular QoS CLI (MQC). Modular CLI is used to configure various QoS features on various Cisco platforms.
- H-QoS: 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.

MPLS TE

The Cisco ASR 9000 Series router supports MPLS TE, this offers the following:

- MPLS TE: 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 Interior Gateway Protocol [IGP] or Label Distribution Protocol [LDP]).

High Availability

The Cisco ASR 9000 Series router is intended for use in 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 or and maximizes availability. The Cisco ASR 9000 Series 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 (minimum disruption restart)
  – Stateful switcheovers
  – In-service software upgrades
  – MPLS TE FRR
  – Bidirectional Forwarding Detection (BFD)
  – Standard IEEE 802.3ad link aggregation bundles

System Configurations

The router runs Cisco IOS XR Software on the following standalone chassis types, available in AC or DC versions:

• a 6-slot chassis
• a 10-slot chassis
Each chassis type supports 40G per slot, and can share route-switch processors (RSPs) and line cards (LCs), which are interchangeable. In each chassis, two slots are designated for RSPs, while the remaining slots accommodate line cards that carry the traffic. The RSPs interconnect the line cards and provide chassis management and control. Any line card can be used as a network-facing trunk card, a subscriber-facing card, or it can provide any other form of connectivity.
The router uses the following line cards:
- 40x1GE Ethernet line card
- 4x10GE Ethernet line card
- 8x10GE Ethernet line card

**Management and Security**

In addition to the management and security features listed below, the router has administrative options, like assigning Task IDs, that control who can perform router tasks.

**Manageability**

- Command-Line Interface—The CLI is a user interface for monitoring and maintaining the router and also for configuring basic router features.
- Simple Network Management Protocol—SNMP is an application-layer protocol that facilitates management information exchange between network devices.
- Trivial File Transfer Protocol—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 synchronizes timekeeping among a set of distributed time servers.
- Cisco IOS XR Software manageability: This feature provides industry-standard management interfaces, including a modular command-line interface (CLI), Simple Network Management Protocol (SNMP), and native XML interfaces.
- 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
  - A flexible common infrastructure for managing network resources
  - Consistent procedures and interfaces for all network elements
Security

- Cisco IOS XR Software: This software provides comprehensive network security features, including ACLs; control-plane protection; routing authentications; authentication, authorization, and accounting (AAA); TACACS+; IP Security (IPSec); Secure Shell (SSH) Protocol; SNMPv3; and leading Routing Policy Language (RPL) support.
- Layer 2 ACLs: You can use this security feature to filter packets under an EVC based on MAC addresses.
- Layer 3 ACLs: This feature matches ACLs by IPv4 protocol packet attributes.
- Security: Many critical security features are supported:
  - 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)
- Authorization, Admission, Accounting (AAA)
- Control Plane Policing (CoPP)

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 need not 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.

Since there are not multiple RSP pairs in this router, the only RSP choices are RSP0 and RSP1. Typically, the lower numbered slot is the chosen RSP. If that RSP is not available the software chooses the RSP in the other slot as the route process controller, making it the primary RSP. During fail over or switch over, 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:

- Telnet
- Secure Shell (SSH)
- Console Server

The router provides different router management interfaces, described in the following sections:
• Command-Line Interface, page 1-10
• Extensible Markup Language API, page 1-10
• Simple Network Management Protocol, page 1-10

Command-Line Interface

The CLI is a user interface for monitoring and maintaining the router and also for configuring basic router features. Through the CLI you execute the Cisco IOS XR commands. All procedures in this guide use CLI. Before you can use other router management interfaces, first use the CLI to install and configure those interfaces. Guidelines for using CLI to configure the router are discussed in the following chapters:

• Chapter 3, “Configuring General Router Features”
• Chapter 4, “Configuring Additional Router Features”
• Chapter 5, “CLI Tips, Techniques, and Shortcuts”

For more CLI procedures, like hardware interface and software protocol management tasks, see the Cisco IOS XR Software documents listed in “Conventions” section on page xii.

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 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, Secure Shell (SSH) and Secure Socket Layer (SSL) transport.

For more information, see the Cisco IOS XR Software documents listed in the “Conventions” section on page xii.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates management information exchange 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, see the Cisco IOS XR Software documents listed in the “Conventions” section on page xii.
Connecting to the Router Through the Console Port

The first time you connect to a new Cisco ASR 9000 Series router with Cisco IOS XR software, 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 afterwards.

---

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>Step 1: Power on the router.</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>This step is required only if the power is not on.</td>
<td></td>
</tr>
<tr>
<td>For information on power installation and controls, see the hardware documentation listed in the “Conventions” section on page xii.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2: Connect a terminal to the Console port.</th>
<th>Establishes a communications path to the router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>During the initial setup, you can communicate with the router only through the Console port.</td>
<td></td>
</tr>
<tr>
<td>The router Console port is designed for a serial cable connection to a terminal or a computer that is running a terminal emulation program.</td>
<td></td>
</tr>
<tr>
<td>The terminal settings are:</td>
<td></td>
</tr>
<tr>
<td>- Bits per second: 9600</td>
<td></td>
</tr>
<tr>
<td>- Data bits: 8</td>
<td></td>
</tr>
<tr>
<td>- Parity: None</td>
<td></td>
</tr>
<tr>
<td>- Stop bit: 2</td>
<td></td>
</tr>
<tr>
<td>- Flow control: None</td>
<td></td>
</tr>
<tr>
<td>For information on the cable requirements for the Console port, see the hardware documentation listed in the “Conventions” section on page xii.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3: Start the terminal emulation program.</th>
<th>(Optional.) Prepares a computer for router communications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The step is not required if you are connecting through a terminal.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4: Press Enter.</th>
<th>Initiates communication with the router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If no text or router prompt appears when you connect to the console port, press Enter to initiate communications.</td>
<td></td>
</tr>
<tr>
<td>If no text appears when you press Enter, give the router more time to complete the initial boot procedure, then press Enter.</td>
<td></td>
</tr>
<tr>
<td>If the prompt gets lost among display messages, press Enter again.</td>
<td></td>
</tr>
<tr>
<td>The router displays the prompt: Username:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Gigabit Ethernet and 10-Gigabit Ethernet Interfaces

After connecting to the router, you need to configure Gigabit Ethernet and Ten Gigabit Ethernet interfaces manually. 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 Gigabit Ethernet and 10-Gigabit Ethernet interfaces.

Where to Go Next

Once you have logged into the router, you are ready to perform general router configuration as described in “CLI Prompt” section on page 3-6.