CHAPTER 1

Introduction to Cisco IOS XR Software

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 CRS Multishelf System Overview, page 1-1
• Cisco CRS Router Overview, page 1-5
• Router Management Interfaces, page 1-11
• Connecting to the Router Through the Console Port, page 1-13
• Where to Go Next, page 1-16

Supported Standalone System Configurations

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

• Cisco CRS 4-Slot Line Card Chassis (LCC)
• Cisco CRS 8-Slot LCC
• Cisco CRS 16-Slot LCC

The Cisco IOS XR software also runs on Cisco CRS Multishelf Systems, which are described in the “Cisco CRS Multishelf System Overview” section on page 1-1.

Cisco CRS Multishelf System Overview

The multishelf system enables multiple Cisco CRS LCCs to act as a single system. This release of the multishelf system supports the following options:

• Two 16-slot LCCs and one, two, or four fabric card chassis (FCCs) to provide a total switching capacity of up to 1.28 Terabits per second (Tbps).
• Three 16-slot LCCs with up to 64 modular services cards (MSCs), and one, two, or four FCCs.
• Four 16-slot LCCs with up to 64 MSCs and one, two, or four FCCs.
- Eight 16-slot LCCs with up to 128 MSCs and one, two, or four FCCs.

Two 22-port shelf controller Gigabit Ethernet (22-port SCGE) cards provide control-plane connectivity among the chassis.

Figure 1-1 shows the single-FCC multishelf system, Figure 1-2 shows the two-FCC multishelf system, and Figure 1-3 shows the four-FCC multishelf system.

**Figure 1-1  Single-FCC Multishelf System**

1. Cisco CRS 16-Slot Line Card Chassis (LCCs)
2. Cisco CRS Fabric Card Chassis (FCCs)
3. 22-port SCGE card (two suggested for each FCC)
Figure 1-2  Two-FCC Multishelf System

1 Cisco CRS 16-Slot Line Card Chassis (LCCs)
2 Cisco CRS Fabric Card Chassis (FCCs)
3 22-port SCGE card (two suggested for each FCC)
Figure 1-3 Four-FCC Multishelf System

1 Cisco CRS 16-Slot Line Card Chassis (LCCs)
2 Cisco CRS Fabric Card Chassis (FCCs)
3 22-port SCGE card (two suggested for each FCC)

For more information on multishelf systems, see Chapter 3, “Bringing Up the Cisco IOS XR Software on a Multishelf System.”
Cisco CRS Router Overview

The Cisco CRS Router is the first carrier router offering continuous system operation, unprecedented service flexibility, and system longevity. This router is powered by Cisco IOS XR software—a unique self-healing, distributed operating system designed for always-on operation while scaling system capacity up to 92 Tbps.

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 triple 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 1-5
- Flexible Ethernet, page 1-7
- L2VPN, page 1-8
- Multicast, page 1-8
- OAM, page 1-9
- Layer 3 Routing, page 1-9
- MPLS VPN, page 1-10
- QoS, page 1-10
- MPLS TE, page 1-11
- Hardware Feature, 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.

- **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.
• Bidirectional Forwarding Detection (BFD)—This protocol has been enhanced to detect connectivity failures over bundle interfaces, which are directly connected between two routers. A benefit of this feature is that problems, such as, link loss or link down, are absorbed by the link aggregation infrastructure. For more information on BFD, see Cisco IOS XR Interface and Hardware Component Configuration Guide for the Cisco CRS Router.

• Lawful Intercept on CRS-3 Line Card—This feature is supported on CRS-MSC-140G and CRS-FP-140 line cards. For more information on Lawful Intercept on CRS-3 Line Card, see the Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router.

• Pseudowire Headend (PWHE)—The pseudowire (PW) virtual interface is a layer 3 interface. This feature supports layer 3 features, such as QoS, along with routing protocols on this interface. For more information on PWHE, see the Cisco IOS XR Modular Quality of Service Configuration Guide for the Cisco CRS Router and the Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco CRS Router.

• 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. The feature also includes VRRP support for IPv6 VRFs and BFD. For more information on VRRP over IPv6, see the Cisco IOS XR IP Addresses and Services Configuration Guide for the Cisco CRS Router.

• In-Service Software Upgrade (ISSU)—In this release, line cards are upgraded using a new procedure called Minimum Disruptive Restart (MDR). For more information on ISSU MDR, see the Cisco IOS XR System Management Configuration Guide for the Cisco CRS Router.

• IPv4 or IPv6 Stateless Translator (XLAT)—This feature enables an IPv4-only endpoint situated in an IPv4-only network to communicate with an IPv6-only endpoint situated in an IPv6-only network. For more information on XLAT, see the Cisco IOS XR Carrier Grade NAT Configuration Guide for the Cisco CRS Router.

• IPv6 Rapid Deployment (6rd)—This is a mechanism that allows a service provider to provide a unicast IPv6 service to customers over an IPv4 network. For more information on 6rd, see the Cisco IOS XR Carrier Grade NAT Configuration Guide for the Cisco CRS Router.

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.
  
  VPLS-specific match criteria, such as match on VPLS-known, match on VPLS-unknown, match on multicast, and match on VPLS-broadcast, are supported.

- **VPLS MAC Address Withdrawal**—For faster VPLS convergence, it is essential to unlearn MAC addresses that have been learned dynamically. This is accomplished by sending an LDP Address Withdraw Message, with the list of MAC addresses to be withdrawn, to all PEs participating in the corresponding VPLS service. Cisco IOS XR supports only wild-card MAC address withdrawal.

- **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 used for interworking two pseudowires together to form a cross-connect relationship.

Multicast

The router supports multicast, which 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 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 Auto RP Lite**—This feature automates the distribution of group-to-RP mappings in a PIM network. This feature has the following benefits:
  - Uses multiple RPs within a network to serve different group ranges.
  - Allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
  - Avoids inconsistent, manual RP configurations that can cause connectivity problems.

- **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.
Multicast VPN Hub and Spoke Support—This feature provides a granular control on the multicast traffic flows through all sites. In this topology, a spoke VRF contains the routes of its own site and the routes of the hub sites. It does not contain the routes of other spokes. Hubs contain the routes of spokes as well as to other hubs. Hub-to-hub connectivity is any-to-any topology.

OAM

The router supports different types of operations, administration, and maintenance (OAM), which 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). This protocol also supports P2MP LSP ping and P2MP LSP Trace Route.

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 IOS XR Routing Configuration Guide for the Cisco CRS Router.

- 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 IOS XR Routing Configuration Guide for the Cisco CRS Router.

- 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 IOS XR Multicast Configuration Guide for the Cisco CRS Router.

- 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 IOS XR Routing Configuration Guide for the Cisco CRS Router.

- 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 IOS XR IP Addresses and Services Configuration Guide for the Cisco CRS Router.

- 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 IOS XR IP Addresses and Services Configuration Guide for the Cisco CRS Router.
• 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 IOS XR Routing Configuration Guide for the Cisco CRS Router.

• ACL-Based Forwarding—This feature lets you specify the next-hop address in ACL configuration. Instead of routing packets based on destination address lookup, the next-hop address specified in ACL configuration is used to forward packets towards the destination. For more information on ACL-Based Forwarding, see the Cisco IOS XR IP Addresses and Services Configuration Guide for the Cisco CRS Router.

• BGP: RT Constrained Route Distribution—This feature is used to reduce the number of unnecessary routing updates that route reflectors (RRs) send to PEs. The reduction in routing updates saves resources. For more information on RT Constrained Route Distribution, see the Cisco IOS XR Routing Configuration Guide for the Cisco CRS-1 Router.

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 OSPFv3, see the Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco CRS Router.

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.

Match on inner VLAN and match on inner cos are supported for both ingress and egress. Set inner cos for both conditional and unconditional marking only in egress are 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 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. 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.

MPLS TE

The router supports MPLS Traffic Engineering (TE), which 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 IGP or LDP).

AutoTunnel Backup—This feature enables a router to dynamically build backup tunnels when they are needed. It eliminates the need for users to pre-configure each backup tunnel and then assign the backup tunnel to the protected interface.

Shared Risk Link Group (SRLG)—A Shared Risk Link Group (SRLG) is a group of network links that share a common physical resource (cable, conduit, node or substructure). An SRLG is identified by a 32-bit number that is unique within an IGP domain. The head end router broadcasts its SRLG and uses it to compute paths.

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 IOS XR MPLS Configuration Guide for the Cisco CRS Router.

Hardware Feature

Multi-rate Copper SFP—This feature adds the speed parameter to the CLI for pluggable copper SFPs. In the Gigabit Ethernet interface configuration, the speed can be configured as:

- Speed {10 | 100 | 1000} (in megabits per second)
- No speed (defaults to 1000)

Router Management Interfaces

Because new routers are not yet configured for your environment, you must begin the configuration using the command-line interface (CLI). This guide provides instructions on using the CLI to configure basic router features. Cisco IOS XR software supports the following router management interfaces, which are described in the following sections:
- Command-Line Interface, page 1-12
- Extensible Markup Language API, page 1-12
- Simple Network Management Protocol, page 1-12

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 Common Object Request Broker Architecture (CORBA). The Secure Socket Layer (SSL) transport is also supported by the XML API.

For more information, 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.

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 “Related Documents” section on page x.

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 on the DSC. Although typical router configuration and management take place using an Ethernet port on the DSC, you must configure the console port for your LAN before it can be used.

Figure 1-4 shows the RP connections on the Cisco CRS 16-Slot LCC, and Figure 1-5 shows the RP connections on the Cisco CRS 4-Slot LCC and Cisco CRS 8-Slot LCC.

Figure 1-4 Communication Ports on the RP for a Cisco CRS 16-Slot LCC
To connect to the router through the Console port, perform the following procedure.

**SUMMARY STEPS**

1. Power on the standalone router, or power on Rack 0 in a multishelf system.
2. Identify the DSC.
3. Connect a terminal to the Console port of the DSC.
4. Start the terminal emulation program.
5. Press Enter.
6. Log in to the router.
7. admin
8. show dsc all

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Power on the standalone router, or power on Rack 0 in a multishelf system.</td>
<td>Starts the router or Rack 0.</td>
</tr>
<tr>
<td></td>
<td>- This step is required only if the power is not on.</td>
</tr>
<tr>
<td></td>
<td>- For information on power installation and controls, see the hardware documentation listed in the “Related Documents” section on page x.</td>
</tr>
<tr>
<td>Step 2 Identify the DSC.</td>
<td>Identifies the RP to which you must connect in the next step.</td>
</tr>
<tr>
<td></td>
<td>- For more information, see the “Connecting to the Router Through the Console Port” section on page 1-13.</td>
</tr>
<tr>
<td>Step 3 Connect a terminal to the Console port of the DSC.</td>
<td>Establishes a communications path to the router.</td>
</tr>
<tr>
<td></td>
<td>- During the initial setup, you can communicate with the router only through the Console port of the DSC.</td>
</tr>
<tr>
<td></td>
<td>- Router Console port is designed for a serial cable connection to a terminal or a computer that is running a terminal emulation program.</td>
</tr>
<tr>
<td></td>
<td>- Terminal settings are:</td>
</tr>
<tr>
<td></td>
<td>- Bits per second: 9600/9600</td>
</tr>
<tr>
<td></td>
<td>- Data bits: 8</td>
</tr>
<tr>
<td></td>
<td>- Parity: None</td>
</tr>
<tr>
<td></td>
<td>- Stop bit: 2</td>
</tr>
<tr>
<td></td>
<td>- Flow control: None</td>
</tr>
<tr>
<td></td>
<td>- For information on the cable requirements for the Console port, see the hardware documentation listed in the “Related Documents” section on page x.</td>
</tr>
<tr>
<td>Step 4 Start the terminal emulation program. (Optional)</td>
<td>(Optional) Prepares a computer for router communications.</td>
</tr>
<tr>
<td></td>
<td>- Not required if you are connecting through a terminal.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
</tbody>
</table>
Where to Go Next

If you have logged into the router or multishelf system, you can perform the general router configuration as described in Configuring General Router Features.

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

If the router is prompting you to enter a root-system username, bring up the multishelf system. For more information, see Chapter 3, “Bringing Up the Cisco IOS XR Software on a Multishelf System”.

### Command or Action | Purpose
--- | ---
**Step 5** 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.
- If the router has no configuration, the router displays the prompt: Enter root-system username:
- If the router has been configured, the router displays the prompt: Username:

**Step 6** Log in to the router. | Establishes your access rights for the router management session.
- Enter the root-system username and password or the username and password provided by your system administrator.
- After you log in, the router displays the CLI prompt, which is described in the “CLI Prompt” section on page 4-83.
- If the router prompts you to enter a root-system username, the router is not configured, and you should follow one of the bring up procedures mentioned in the next section.

**Step 7** admin | Places the router in administration EXEC mode.

**Example:**
RP/0/RP0/CPU0:router# admin

**Step 8** show dsc all | Displays the DSC information for the router or router system so that you can verify that you have connected to the DSC console port.

**Example:**
RP/0/RP0/CPU0:router(admin)# show dsc all