Cisco IOS XR Fundamentals

Mobeen Tahir • Mark Ghattas
Dawit Birhanu • Syed Natif Nawaz

ciscopress.com

Cisco IOS XR Fundamentals

Mobeen Tahir, Mark Ghattas, Dawit Birhanu, Syed Natif Nawaz

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing June 2009

Library of Congress Cataloging-in-Publication Data:

Cisco IOS XR fundamentals / Mobeen Tahir ... [et al.].

p. cm.

Includes bibliographical references.

ISBN-13: 978-1-58705-271-2 (pbk.)

ISBN-10: 1-58705-271-7 (pbk.)

1. Cisco IOS. 2. Routing (Computer network management) 3. Routers (Computer networks)
4. Internetworking (Telecommunication) I. Tahir, Mobeen, 1966- II. Cisco Systems, Inc. III. Title.

TK5105.8.C57C548 2009

004.6—dc22

2009019283

ISBN-13: 978-1-58705-271-2

ISBN-10: 1-58705-271-7

Warning and Disclaimer

This book is designed to provide information about the Cisco IOS XR network operating system. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Development Editor: Dayna Isley

Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Ken Johnson

Business Operation Manager, Cisco Press: Anand Sundaram

Manager Global Certification: Erik Ullanderson

Copy Editor: Mike Henry

Technical Editors: Mukhtiar Shaikh, Syed Kamran Raza

Proofreader: Leslie Joseph

Foreword

Over the last several years, fiscal discipline has really dominated the industry. Both consumers and businesses expect far more from their communications providers than they did just a few years ago. Offering simple telephone dial tone and an Internet connection are not going to be enough for success. At the same time, however, service providers want to continue to reduce their operational costs. As a result, one of the main challenges telecommunications companies now face is to find ways to cost effectively bring innovative services to their customers. These drivers are why most providers are working on transitioning their disparate legacy networks to one, unified, converged network infrastructure based on IP combined with Multiprotocol Label Switching (MPLS). MPLS is a technology that translates various other telecommunications protocols, such as ATM or frame relay, so they can run over an IP-based network. By eliminating their multiple networks, service providers are greatly reducing their operational costs. And by moving to an IP/MPLS network, they can mix and match all communications types—voice, data, and video—into any service their customers might want.

We believe the CRS-1 will dramatically affect carriers and their capability to successfully transition to this new era in communications. Carriers worldwide are embracing convergence and almost unanimously agree that IP/MPLS is the foundation for their new infrastructures. The CRS-1 provides carriers the means to consolidate their networks in the most efficient and cost-effective way possible. Nothing on the market can match it in terms of scalability, reliability, and flexibility. It is a system that our service provider customers will be able to base their businesses on. And I firmly believe that carriers that deploy the CRS-1 will gain profound competitive advantage over their competition through operational efficiencies and service flexibility. As we like to point out, when service providers work with Cisco, they are not just working with a network equipment maker but, rather, a business partner.

Sameer Padhye
Sr. Vice President, Advanced Services
WW Service Provider Line of Business
Customer Advocacy

Introduction

This book is intended to provide a reference to users who plan or have implemented Cisco IOS XR software in the network. *Cisco IOS XR Fundamentals* provides an overview of IOS XR operation system infrastructure and hardware architecture on the Carrier Routing System. The intention of this book is to provide general networking topics in IOS XR that service providers may implement in the core network. It is not feasible to cover every aspect of IOS XR; however, the key configurations have been explained that are typically deployed in core networks.

Who Should Read This Book?

Readers who have a relatively strong working knowledge of Cisco IOS Software and routing protocols will benefit from the discussions and configuration examples presented.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to provide a configuration overview on Cisco IOS XR to support implementation configuration and features in IOS XR. Chapter 1 provides an overview of the evolution of operating systems and an understanding of the underlying QNX operating system. Chapters 2 through 12 are the core chapters and can be covered in order. If you do intend to read them all, the order in the book is an excellent sequence to use.

Chapters 1 through 12 cover the following topics:

- **Chapter 1, "Introducing Cisco IOS XR":** This chapter discusses the evolution of network operating systems in service provider enviroments. It is important to understand the goals and requirement of service providers that influenced the goals of IOS XR.
- **Chapter 2, "Cisco IOS XR Infrastructure":** This chapter discusses the interworkings of IOS XR. It helps you understand IOS XR microkernel architecture, process scheduling, interprocess communications, system database, and distributed services.
- **Chapter 3, "Installing Cisco IOS XR":** This chapter discusses various procedures for installing IOS XR on the Carrier Routing System.
- **Chapter 4, "Configuration Management":** This chapter provides a deeper insight into how IOS XR is different when configuring interfaces, out of band management, and features such as rollback and commit commands. Understanding these features will help you better manage the system.
- **Chapter 5, "Cisco IOS XR Monitoring and Operations":** This chapter explores how monitoring works in IOS XR. As IOS XR operates as a real-time operating system, there are monitoring tools that provide deeper inspection of activities on the system.
- **Chapter 6, "Cisco IOS XR Security":** This chapter examines inherent policers that provide a layer of security within the operating system. The importance of Local Packet Transport System (LPTS) is discussed.

- **Chapter 7, "Routing IGP":** This chapter covers the basics of routing protocol configurations. It provides configuration examples to show how IGP features are configured in IOS XR.
- **Chapter 8, "Implementing BGP in Cisco IOS XR":** This chapter introduces the IOS XR implementation of BGP. This chapter assumes that you have prior experince and knowledge of the BGP protocol and focuses on unique aspects of IOS XR BGP configuration. This chapter also provides details on Routing Policy Language as a vehicle for implementing BGP routing policies.
- **Chapter 9, "Cisco IOS XR MPLS Architecture":** This chapter discusses Multiprotocol Label Switching (MPLS), an important technology for building converged network infrastructure and services. This chapter assumes that you are familiar with MPLS protocols and operations. This chapter discusses IOS XR MPLS architecture, features, implementation, and configuration. It covers LDP, Layer 3 VPN, VPWS, VPLS, and MPLS Traffic Engineering.
- **Chapter 10, "Cisco IOS XR Multicast":** This chapter discusses when to use queuing and which queuing technique to use. This chapter also examines Weighted Fair Queuing (WFQ), Custom Queuing, and Priority Queuing and addresses the need for compression in today's enterprise network.
- **Chapter 11, "Secure Domain Router":** This chapter covers the concept of SDRs. It discusses the Distributed Route Processor (DRP) hardware needed to implement SDRs and provides configuration examples.
- **Chapter 12, "Understanding CRS-1 Multishelf":** This chapter discusses the Cisco implementation of the CRS-1 multishelf system. The key components are discussed to understand the architecture and troubleshooting of a CRS-1 multishelf system. A fabric troubleshooting section is covered to support implementation and operation.

CHAPTER 6

Cisco IOS XR Security

It is important to control access to the router to prevent unauthorized or malicious use that might take the router offline or use it to launch an attack on the rest of the network. Cisco IOS XR provides the authentication, authorization, and accounting (AAA) framework that helps provide secure access via the logical vty and the physical tty ports. Furthermore, ensuing sections in this chapter discuss the concepts of task-based authorization and familiarize the user with IOS XR concepts such as admin and SDR planes as well as the uniqueness of user groups and task group configuration.

Forwarding plane refers to the components involved in the various stages during packet forwarding. Forwarding plane refers not only to the flow of a packet through the router but also to the packets destined to the router. Protection of forwarding plane is important and necessitates controlling the type of traffic that traverses the router, and limiting the amount of traffic that's destined to the router itself so that the router does not become a victim of a denial of service (DoS) attack. You might well be familiar with access control lists (ACL) and Unicast Reverse Path Forwarding (uRPF) as popular forwarding plane security features. Additionally, IOS XR has a concept of Local Packet Transport Service (LPTS). LPTS provides protection against traffic destined to the router. This type of traffic is usually related to routing protocols that typically run on the route processor (RP) of the router, though Telnet, SNMP, NTP, ping, traceroute, and various other services create traffic that can be destined to a router's line card or RP CPU. This chapter discusses the details behind LPTS and highlights key elements of forwarding plane security.

Secure Operating System

A router running IOS XR is often used as a backbone router providing core routing capabilities. Cisco IOS XR might also be used on a provider edge router provisioned with edge services such as Layer 2 and Layer 3 VPNs, QoS, and so on. Architectures such as IOS XR often play a critical role in a service provider (SP) network as a core or an edge device, and its security needs are a paramount concern for the network administrator.

Figure 6-1 shows a visual representation of IOS XR secure software design. IOS XR is a microkernel-based operating system. All essential services, such as TCP, UDP, and driver software, run as an independent application on top of its microkernel. Any individual application-level disaster remains contained and has minimal chances of interfering with the core functions of the operating systems. This makes IOS XR internals safe and less vulnerable to exploitation.

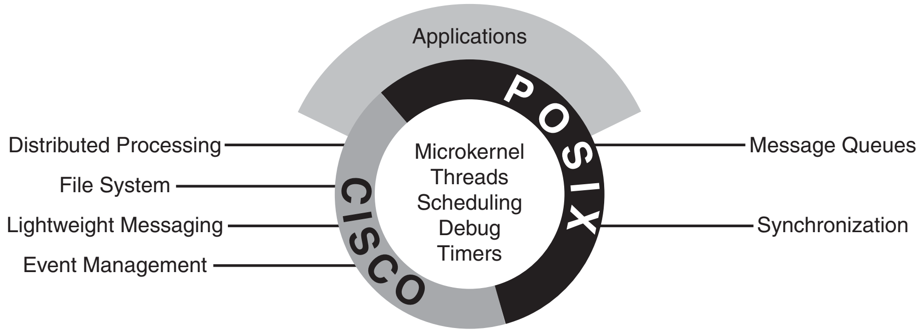

Figure 6-1 *Secure Software Design*

Cisco IOS XR processes run in their own memory space and are "restartable" by design. The software design takes preemptive measures against denial of service–type attacks. IOS XR also mitigates out-of-resource conditions and makes the continuous operation of the system more reliable.

Figure 6-1 illustrates the following main points:

- IOS XR is a microkernel-based operating system offering memory protection and fault tolerance.
- All basic OS and router functionality is implemented as processes. All the distributed services run on top of the microkernel.
- IOS XR follows a UNIX process model with separate, protected memory address spaces for its processes. The microkernel is protected from faults occurring in the protocol or device driver software due to the layered model shown in the figure.

Despite the inherent built-in security and high availability in the operating system, certain configuration measures are inevitable to ensure router and network security. Ensuing sections in this chapter delve deeper into the security considerations of a router or a network of devices running on IOS XR.

Securing Access to the Router

You can access an IOS XR router by using the physical console and auxiliary ports or using the logical vty ports. The console port helps create a terminal session with the router using the standard RS-232 asynchronous serial communications using a commonly found RJ-45 connection. Console ports help configure the router for the first time when it has no configuration and it is advisable to maintain a console connection to the router to aid in debugging or disaster recovery. The auxiliary (aux) port natively runs the Korn Shell (ksh) as its mode of operation. In addition to the physical asynchronous serial ports, IOS XR natively supports router access through 100 vty ports from the range 0 to 99. Furthermore, IOS XR by default enables vty ports in the range 100 to 106 for the embedded event manager (EEM) scripts. This section talks about the access security of the router using local and external AAA.

Note: The IOS XR command **telnet ipv4 server max-servers** is used to limit the number of simultaneous users that can access the router.

AAA authentication commands are defined in Cisco IOS XR to verify a user who attempts to access the system. Cisco IOS XR performs authentication by comparing the incoming user ID and password with what is stored in a security database.

AAA authorization is supported in Cisco IOS XR. It maintains the capability to create audit trails by recording user's actions if specified to do so in Cisco IOS XR.

AAA accounting is the process of tracking user activity and the amount of resources being consumed. Cisco IOS XR provides a method of collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, and the executed commands on the router. Cisco IOS XR software supports both the TACACS+ and RADIUS methods of accounting.

Cisco IOS XR operating software maintains two resource management planes from a router access perspective:

- Admin plane
- Secure domain router (SDR) plane

The admin plane consists of resources shared across all secure domain routers. On the other hand, the SDR plane consists of those resources specific to the particular SDR.

IOS XR router security involves concepts of user and task groups. The concepts of user group, task group, and inheritance are important for the understanding of command permissions. These topics will be discussed in more detail later in this chapter. External AAA using TACACS+ and RADIUS are standard access security features. These features will also be illustrated with configuration examples in future sections of this chapter. Configuration examples are provided for Secure Shell (SSH) configurations along with useful show commands.

IOS XR MPP provides the network administrator with the flexibility to restrict interfaces on which network management packets are allowed to enter a device. MPP discussion and examples are a forthcoming topic in this chapter.

Admin Plane

The admin plane maintains responsibility for the owner SDR, and certain administrative responsibilities for all other nonowner SDRs. These functions include user control over power, fan-trays, fabric modules, and environmental aspects of the router required to maintain normal operations. The admin plane is accessible only to a type of user known as the *root-system user*. IOS XR requires configuration of a root-system user using the initial setup dialog. IOS XR router does not allow the system to operate without a user group configuration. If all users and external AAA configurations get deleted, IOS XR prompts the next logged-in user for a new username and password.

SDR Plane

As mentioned in the preceding section, the root-system user has the highest level of privilege for the router operation. This user has the ability to provision SDRs and create root SDR users. After being created, root-lr (the abbreviation *lr* in *root-lr* stands for *logical router*) users take most of the responsibilities from the root-system user for the SDR. The root-lr user is the equivalent of root-system user from an SDR perspective and has jurisdiction only for the particular SDR on which it is defined. A detailed discussion of SDR plane is included in Chapter 11, "Secure Domain Router."

User Groups and Task Groups

Before getting into the details of AAA configuration, this section acquaints you with the concepts of user groups, task groups, and task IDs. The user group concept in IOS XR relates to a group of users with common characteristics. A user that logs in to an IOS XR router may have one or more preconfigured user groups assigned to it. Some user groups are precreated by default and others may be defined via configuration. Table 6-1 lists the predefined user and task groups in IOS XR.

Table 6-1 *Predefined User Groups*

User Groups and Task Groups	Purpose
cisco-support	Used by Cisco Support Team. Provides access to troubleshooting commands.
netadmin	Provides the ability to control and monitor all system- and network-related parameters.
operator	Provides very basic user privileges.
root-lr	Provides the ability to control and monitor the specific SDR.
root-system	Provides the ability to control and monitor the entire system.
sysadmin	Provides the ability to control and monitor all system parameters but cannot configure network protocols.
serviceadmin	Provides the ability to administer session border controllers.

Note: The useful AAA command **show aaa task supported** lists all the available tasks that can be used to select the correct task authorization.

In addition to the predefined task groups, IOS XR provides the ability to custom create task groups consisting of individual tasks. Tasks, in turn, contain a collection of task IDs that define actions such as READ, WRITE, EXECUTE, or DEBUG (R/W/E/D).

The following list elaborates the R/W/E/D task IDs:

- **R:** Permits only a read operation

- **W:** Permits a change (or write) operation and allows an implicit read
- **E:** Permits an access operation (or execution), such as ping or Telnet
- **D:** Permits a debug operation

The concept of tasks, task groups, and task IDs might sound confusing. An example can elucidate this new concept. Suppose a network administrator wants to create a user group called igp-admin that has the capability to execute the following tasks:

- Run **debug** commands for bundle interfaces
- Carry out all configuration and monitoring tasks related to OSPF
- Run only **debug** and **show** commands for MPLS TE

Example 6-1 illustrates the steps needed to meet the preceding requirements.

Example 6-1 *Creating User Groups and Task Groups*

```
! A taskgroup igp-admin is created, the following show command depicts the task-
  group igp-admin
!
RP/0/RP0/CPU0:CRS1-1#show running-config taskgroup igp-admin
taskgroup igp-admin
 task read ospf
 task read mpls-te
 task write ospf
 task execute ospf
 task debug ospf
 task debug bundle
 description OSPF Administrator
! Create a usergroup called igp-admin
RP/0/RP0/CPU0:CRS1-1(config)#usergroup igp-admin
RP/0/RP0/CPU0:CRS1-1(config-ug)#taskgroup igp-admin
RP/0/RP0/CPU0:CRS1-1(config-ug)#commit
RP/0/RP0/CPU0:CRS1-1(config-ug)#exit
!
! Use the following show command to verify the user-group igp-admin
RP/0/RP0/CPU0:CRS1-1#show running-config usergroup igp-admin
usergroup igp-admin
 taskgroup igp-admin
!
! Create a username called igpadmin and configure a secret
RP/0/RP0/CPU0:CRS1-1(config)#username igpadmin
RP/0/RP0/CPU0:CRS1-1(config-un)#group igp-admin
RP/0/RP0/CPU0:CRS1-1(config-un)#secret cisco
RP/0/RP0/CPU0:CRS1-1(config-un)#commit
!
! The following show command verifies the creation of the user-group igpadmin
!
```

```
RP/0/RP0/CPU0:CRS1-1#show running-config username igpadmin
username igpadmin
 secret 5 $1$JodH$mJSA9cRx5IiISitvvOywU.
 group igp-admin
!
```

Example 6-1 creates a task group called igp-admin and assigns the task IDs READ, WRITE, EXECUTE, and DEBUG for OSPF and only READ capability for MPLS-TE and DEBUG capability for bundle tasks, respectively.

A user group called igp-admin is created that references the task group igp-admin. A local AAA username configuration is created that assigns the user group igp-admin to username igpadmin. The username igpadmin is configured with a secret password for authentication purposes. IOS XR supports both a clear text password and a one-way encrypted secret. Using the one-way encrypted secret is ideal for the application shown in Example 6-1.

Example 6-2 demonstrates the **describe** command that can be used to determine the right authorizations if some useful tasks are found to be missing. A user logs in to the router and tries to execute the **show route summary** command only to realize that the command cannot be executed due to missing task authorizations. The **describe** command reveals that the RIB (READ) privilege is required before **show route summary** can be executed.

Example 6-2 *Determining the Right Task ID for an Operation*

```
! Telnet to the router to verify the new configuration. IP address 192.168.254.1
  is that ! of the router on which the new user igpadmin was created.
RP/0/RP0/CPU0:CRS1-1#telnet 192.168.254.1
Trying 192.168.254.1...
Connected to 192.168.254.1.
Escape character is '^^'.
Username: igpadmin
Password:
!
!
RP/0/RP0/CPU0:CRS1-1#show user
igpadmin
! The following command verifies the newly created tasks and their task IDs
RP/0/RP0/CPU0:CRS1-1#show user tasks
Task:                bundle  :                                DEBUG
Task:               mpls-te  : READ
Task:                  ospf  : READ    WRITE    EXECUTE    DEBUG
! Try executing a routing related show command
RP/0/RP0/CPU0:CRS1-1#show route summary
% This command is not authorized
! It appears that an important show command that this user
! needs is not working due to the lack of the right authorization.
```

```
! The "describe" command can be used to find out why this command may not have
! worked, though  to execute the describe command the user logs in again
! with privileges root-system and cisco-support.
!
RP/0/RP0/CPU0:CRS1-1#describe show route
The command is defined in ip_rib_cmds.parser
Node 0/RP0/CPU0 has file ip_rib_cmds.parser for boot package /disk0/hfr-os-mbi-
  3.6.0/mbihfr-rp.vm from hfr-base
Package:
    hfr-base
        hfr-base V3.6.0[00]  Base Package
        Vendor : Cisco Systems
        Desc   : Base Package
        Build  : Built on Mon Dec 17 09:25:24 PST 2007
        Source : By edde-bld1 in /auto/srcarchive2/production/3.6.0/hfr/workspace
         for c2.95.3-p8
        Card(s): RP, DRP, DRPSC, OC3-POS-4, OC12-POS, GE-3, OC12-POS-4, OC48-POS,
  E3-OC48-POS, E3-OC12-POS-4, E3-OC3-POS-16, E3-OC3-POS-8, E3-OC3-POS-4, E3-OC48-
  CH, E3-OC12-CH-4, E3-OC3-CH-16, E3-GE-4, E3-OC3-ATM-4, E3-OC12-ATM-4, E5-CEC,
  E5-CEC-v2, SE-SEC, LC, SP, SC
        Restart information:
          Default:
            parallel impacted processes restart
Component:
    ip-rib V[main/217]  Generic RIB infrastructure
File:
    ip_rib_cmds.parser
        Card(s)              : RP, DRP, SC
        Local view           : /pkg/parser/ip_rib_cmds.parser
        Local install path   : /disk0/hfr-base-3.6.0/parser/ip_rib_cmds
User needs ALL of the following taskids:
        rib (READ)
It will take the following actions:
  Spawn the process:
        show_ipv4_rib -X 0x1 -Y 0x1 -Z ________ -s ipv4 ________
!
! From the highlighted output it is obvious that to
! use "show route" command the task rib must have
! TaskID (READ)
!
! The output of the describe command indicates
! that the tasked "rib (READ)" is required.
!
RP/0/RP0/CPU0:CRS1-1(config)#taskgroup igp-admin
```

```
RP/0/RP0/CPU0:CRS1-1(config-tg)#task read rib
RP/0/RP0/CPU0:CRS1-1(config-tg)#task execute rib
RP/0/RP0/CPU0:CRS1-1(config-tg)#task write rib
RP/0/RP0/CPU0:CRS1-1(config-tg)#task debug rib
RP/0/RP0/CPU0:CRS1-1(config-tg)#commit
RP/0/RP0/CPU0:CRS1-1(config-tg)#exit
!
! A show command showing the newly modified taskgroup
!
RP/0/RP0/CPU0:CRS1-1#show running-config taskgroup igp-admin
taskgroup igp-admin
 task read rib
 task read ospf
 task read mpls-te
 task write rib
 task write ospf
 task execute rib
 task execute ospf
 task debug rib
 task debug ospf
 task debug bundle
 description OSPF Administrator
!
! Login to the router once again to verify the new settings
RP/0/RP0/CPU0:CRS1-1#telnet 192.168.254.1
Trying 192.168.254.1...
Connected to 192.168.254.1.
Escape character is '^^'.
Username: igpadmin
Password:
! show user command shows the new rib task
RP/0/RP0/CPU0:CRS1-1#show user
Igpadmin
RP/0/RP0/CPU0:CRS1-1#show user tasks
Task:                bundle  :                              DEBUG
Task:               mpls-te  : READ
Task:                  ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                   rib  : READ    WRITE    EXECUTE    DEBUG
!
!show route command can now be executed as the
! authorization issue stands resolved
RP/0/RP0/CPU0:CRS1-1#show route summary
Route Source    Routes    Backup    Deleted    Memory (bytes)
connected       11        5          0           2176
local           16        0          0           2176
```

```
ospf 1          5        0        0          680
isis xr         4        4        0          1216
static          2        0        0          272
bgp 102         0        0        0          0
local SMIAP     1        0        0          136
Total           39       9        0          6656
```

User Group and Task Group Inheritance

User groups and task groups can inherit from other user groups and task groups, respectively. If task group X inherits from task group Y, task group X contains the attributes of X as well as those of Y. In other words, this inheritance produces a "union" of two task groups. The same concept is true for user groups.

Example 6-3 helps illustrate the concept of inheritance. Consider the user group igpadmin created in the previous example. A new user group is created and named deb-eigrp. The user group deb-eigrp has been assigned the debug task for the EIGRP protocol.

Example 6-3 *User Group Inheritance*

```
usergroup igpadmin
 taskgroup igp-admin

! The example shows a user called igpadmin that uses the usergroup igpadmin
username igpadmin
 group igpadmin
 secret 5 $1$laNp$2s/dTtBkqvfkB01B9wqft/

! User igpadmin logs into the router as shown:
RP/0/RP1/CPU0:CRS-1#telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Username: igpadmin
Password: cisco

! After logging into the router the user checks his tasks with the "show user
! tasks" command.
RP/0/RP1/CPU0:CRS-1#show user tasks
Fri Mar 20 10:26:01.356 PST
Task:                bundle  :                               DEBUG
Task:               mpls-te  : READ
Task:                  ospf  : READ     WRITE     EXECUTE     DEBUG
Task:                   rib  : READ     WRITE     EXECUTE     DEBUG



! Now a new usergroup called deb-eigrp is created that uses the taskgroup
! debug-eigrp.
```

```
! This configuration is carried out the network administrator and not the
! igpadmin user.
 RP/0/RP1/CPU0:CRS-1#show run taskgroup debug-eigrp
Fri Mar 20 10:31:44.150 PST
taskgroup debug-eigrp
 task debug eigrp
!
 usergroup deb-eigrp
 taskgroup debug-eigrp
!
The administrator assigns the usergroup deb-eigrp to usergroup igpadmin by way of
 inheritance.
usergroup igpadmin
 taskgroup igp-admin
 inherit usergroup deb-eigrp
!
! The user igpadmin logs again into the router and executes the command "show
! user tasks". Note that inheritance has allowed eigrp debug capability to be
! added to the user igpadmin.
RP/0/RP1/CPU0:CRS-1#telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.

Username: igpadmin
Password: cisco  Mar 18 07:59:33 2009: 2 days, 2 hours, 34 minutes ago

RP/0/RP1/CPU0:CRS-1#show user tasks
Fri Mar 20 10:33:50.893 PST
Task:              bundle  :                                DEBUG
Task:               eigrp  :                                DEBUG
Task:             mpls-te  : READ
Task:                ospf  : READ     WRITE     EXECUTE     DEBUG
Task:                 rib  : READ     WRITE     EXECUTE     DEBUG

RP/0/RP1/CPU0:CRS-1#
```

Let us use another example to demonstrate the concept of inheritance in task groups. A new task group is being created for the user mplsadmin. The requirements for this user are as follows:

- READ, WRITE, EXECUTE, and DEBUG task IDs for MPLS TE
- All the attributes of task group igp-admin

Example 6-4 creates the new task group using inheritance from the already existing task group called igp-admin that was created in Example 6-3.

Example 6-4 *Determining the Right Task ID for an Operation*

```
RP/0/RP1/CPU0:CRS1-1(config)#taskgroup mpls-admin
RP/0/RP1/CPU0:CRS1-1(config-tg)#task debug mpls-te
RP/0/RP1/CPU0:CRS1-1(config-tg)#task execute mpls-te
RP/0/RP1/CPU0:CRS1-1(config-tg)#task read mpls-te
RP/0/RP1/CPU0:CRS1-1(config-tg)#task write mpls-te
RP/0/RP1/CPU0:CRS1-1(config)#inherit taskgroup igp-admin
RP/0/RP1/CPU0:CRS1-1(config-tg)#commit
RP/0/RP1/CPU0:CRS1-1(config-tg)#exit
!
! Use the following show command to verify the configuration from the previous task
RP/0/RP1/CPU0:CRS1-1#show running-config taskgroup mpls-admin
taskgroup mpls-admin
 task read mpls-te
 task write mpls-te
 task execute mpls-te
 task debug mpls-te
 inherit taskgroup igp-admin
!
```

External AAA

Cisco IOS XR supports external AAA using standard IP-based protocols such as TACACS+ and RADIUS. TACACS+ and RADIUS protocols can be used in conjunction with a product such as the Cisco Secure Access Control Server (ACS) to provide an external AAA database. The following describes some key elements of AAA configuration:

- The security server and client are identified by IP addresses and a secret shared key is configured between them.
- The notion of a user group on IOS XR local AAA is unrelated to a user group on an ACS server. The configuration of user groups on the ACS server is a separate ACS-only feature.
- IOS XR task groups are identified as optional attributes on the ACS server. Two methods exist that can help identify task IDs remotely. The first method uses the concept of task maps and the second uses the privilege levels.

Example 6-5 demonstrates the external configuration for tasks. Note that these configurations are on the server side of external AAA and not on the router.

Example 6-5 *Task Configuration Semantics on an External Server*

```
user = igpadmin{
       member = igp-admin-group
       opap = cleartext "cisco"
       service = exec {
       task = "rwxd:ospf,#operator"
       }
}
```

Example 6-5 specifies the task ID as an attribute in the external TACACS+ or RADIUS server. Note that this is shown as an example only. Because the procedure can vary from server to server, consult the TACACS+ or RADIUS server documentation to find out how you can use the optional attributes. A freeware TACACS+ server from Cisco might require an asterisk (*) instead of an equal sign (=) before the attribute value for optional attributes. Example 6-5 shows the task string in the configuration file of the TACACS+ server where tokens are delimited by a comma (,). Each token contains either a task ID name or its permissions in the following format:

```
task = "<permissions>:<taskid name>, #<usergroup name>, ..." .
```

In Example 6-5, the task = "rwxd:ospf,#operator" assigns READ, WRITE, EXECUTE, and DEBUG task IDs to the OSPF task and assigns the user group operator.

Example 6-6 is quoted from Cisco.com and demonstrates the ability to interact with a TACACS+ daemon that does not have the concept of task IDs. In this case a privilege-level mapping is used.

Example 6-6 *Privilege-Level Mappings*

```
!
! TACACS+ example
!
user = admin1{
    member = bar
    service = exec-ext {
        priv_lvl = 5
    }
}
!
!RADIUS Example using Cisco AV-pair
!
user = admin2{
    member = bar
    Cisco-AVPair = "shell:tasks=#root-system,#cisco-support"{
        Cisco-AVPair = "shell:priv-lvl=10"
    }
}
```

Cisco IOS XR AAA supports a mapping between privilege levels that can be defined for a given user in the external TACACS+ server file. The local user group on the router needs to be configured with a user group with a name that matches the privilege level. After TACACS+ authentication, the user gets assigned the task map of the user group mapped to the privilege level received from the external TACACS+ server. Example 6-6 shows a TACACS+ configuration followed by a RADIUS configuration. If the IOS XR router is configured with local user groups priv5 and priv10, they can be mapped to the privilege levels 5 and 10 configured for TACACS+ and RADIUS, respectively. Privilege levels from 1 to 13 may be used in a similar way. Privilege level 15 maps to the root-system and privilege level 14 maps to root-lr.

The following sections discuss the configuration behind external AAA. Various CLI command options for configuring TACACS+ are presented.

Configuring a TACACS+ Server

Figure 6-2 shows an IOS XR router connected to an ACS server. Example 6-7 creates a simple TACACS+ configuration using an external ACS server with an IP address of 172.18.172.16.

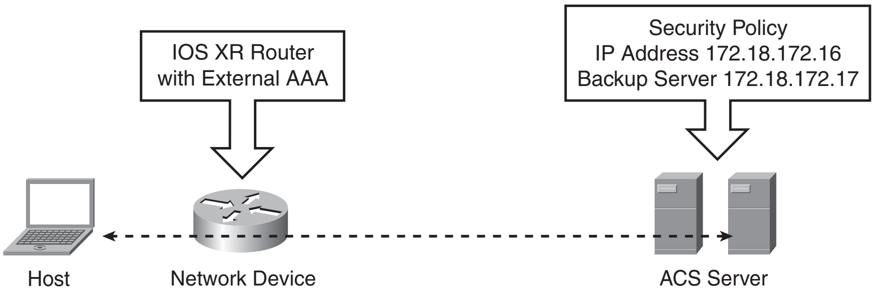

Figure 6-2 *Authentication with an External AAA Server*

Example 6-7 *Configuring AAA with an External TACACS+ Server*

```
RP/0/RP0/CPU0:CRS-A#show run aaa
usergroup priv11
taskgroup netadmin
taskgroup igpadmin
!
tacacs-server host 172.18.172.16 port 49
tacacs-server key 7 06150E2F46411A1C
tacacs source-interface MgmtEth0/0/CPU0/0
!
aaa group server tacacs+ chap6
 server 172.18.172.17
!
aaa authentication login console local
aaa authentication login chap-6 group chap6 local
aaa default-taskgroup root-system
!
line template lab
 login authentication chap-6
 exec-timeout 30 0
!
line console
 login authentication console

vty-pool default 0 99 line-template lab
```

In Example 6-7, a privilege 11 configuration exists on the ACS server. The AAA server is identified with the **tacacs server host** command and a backup server is identified with the **aaa group server** command. The **local** keyword in the **aaa authentication login chap-6 group chap6 local** command ensures that AAA will authenticate locally in the case of failure of both the ACS servers. The AAA method list chap-6 gets assigned to the vty pool.

Authentication Using RADIUS

This section shows some configuration examples for AAA RADIUS client configuration on IOS XR to allow authentication with an external ACS server.

Example 6-8 shows a basic AAA RADIUS configuration. The basic concept is the same as that shown in Example 6-7 except the TACACS+ protocol has been replaced by RADIUS.

Example 6-8 *Configuring AAA with an External RADIUS Server*

```
RP/0/RP0/CPU0:CRS-B_IOX#show run aaa
usergroup priv13
 taskgroup root-system
 taskgroup cisco-support
!
radius-server host 172.18.172.16
 key 7 104D000A0618
!
radius source-interface MgmtEth0/RP0/CPU0/0
aaa authentication login telnet group radius local
aaa authentication login default local
!
line template rads
 login authentication telnet
 exec-timeout 0 0
 session-timeout 0
vty-pool default 0 99 line-template rads
telnet ipv4 server max-servers no-limit
```

Example 6-9 shows AAA RADIUS authentication and introduces a new authorization command: **aaa authorization exec default none**. This command has the same effect as the keyword **if-authenticated** in IOS AAA authorization commands. The configuration states that if a user is authenticated, that user is also authorized.

Example 6-9 *AAA with an External RADIUS Server with Accounting and Authorization*

```
! Configures Radius server dead times and dead-criteria
!
radius-server deadtime 1
radius-server dead-criteria time 15
radius-server dead-criteria tries 2
```

```
!
! Configures the RADIUS server hosts
!
aaa group server radius XR-GROUP
 server 172.18.172.16 auth-port 1645 acct-port 1646
 server 172.18.172.17 auth-port 1645 acct-port 1646
!
! Enables AAA accounting
aaa accounting exec default start-stop group XR-GROUP
aaa accounting commands default start-stop group XR-GROUP
!
! Configure authorization to occur automatically if the user gets authenticated
!
aaa authorization exec default none
!
! sets login authentication to use the default method list and XR-GROUP server
aaa authentication login default group XR-GROUP local
end
```

Configuring Secure Shell

Secure Shell (SSH) is a useful protocol or application for establishing secure sessions with the router. A router configured with SSH server allows a secure connection to the router similar to Telnet. The Telnet application has limited security. SSH provides stronger encryption and deploys public-key cryptography for added confidentiality. SFTP also comes as a component of SSH and enables secure FTP (SFTP) capabilities for downloading software or configuration files. IOS XR supports two versions of SSH:

- SSH version 1 uses Rivest, Shamire, and Adelman (RSA) keys.
- SSH version 2 uses the Digital Signature Algorithm (DSA).

Enabling SSH on IOS XR requires the Hfr-k9sec security PIE to be installed on the router. In addition to installing the k9sec PIE, IOS XR requires RSA or DSA keys to be generated on the router before SSH runs in server mode. Example 6-10 illustrates the SSH configuration on IOS XR.

Example 6-10 *Enabling SSH v2 on IOS XR*

```
!
!The command below verifies the existence of k9sec pie
!
RP/0/RP1/CPU0:CRS1-1(admin)#show install active ¦ include k9sec
      disk0:hfr-k9sec-3.6.0
!
! The following command generates DSA key pairs
!
RP/0/RP1/CPU0:CRS1-1#crypto key generate dsa
```

```
The name for the keys will be: the_default
  Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024
    bits. Choosing a key modulus
How many bits in the modulus [1024]: 1024
Generating DSA keys ...
Done w/ crypto generate keypair
[OK]
!
RP/0/RP1/CPU0:CRS1-1(config)#ssh server v2
RP/0/RP1/CPU0:CRS1-1(config)#commit
```

In Example 6-10 the presence of the k9sec PIE is verified first. If this PIE is not present, it needs to be installed. The example shows the generation of DSA keys by executing the **crypto key generate dsa** command, followed by enabling SSH version 2 in Configuration mode.

Example 6-11 demonstrates the debugging of SSH server functionality on a router with the **debug ssh server** command followed by the **show ssh session detail** command.

Example 6-11 *Debugging SSH v2 on IOS XR*

```
! Enable ssh server debugging on the router
!
RP/0/RP1/CPU0:CRS1-1#debug ssh server
RP/0/RP1/CPU0:CRS1-1#show debug
####  debug flags set from tty 'vty0'  ####
ssh server flag is ON
!
! Create an SSH session from a unix server to the IOS XR router
!
$ ssh cisco@10.10.20.31
Password:cisco
Last switch-over Sun Jun  1 08:51:09 2008: 2 weeks, 3 hours, 27 minutes ago
RP/0/RP1/CPU0:CRS1-1#RP/0/RP1/CPU0:Jun 15 12:18:50.284 : SSHD_[364]: Spawned new
  child process 6852847
RP/0/RP1/CPU0:Jun 15 12:18:50.482 : SSHD_[65775]: Client sockfd 3
RP/0/RP1/CPU0:Jun 15 12:18:50.494 : SSHD_[65775]: Connection from 10.10.20.100
  port 61532
RP/0/RP1/CPU0:Jun 15 12:18:50.517 : SSHD_[65775]: Session id 0
RP/0/RP1/CPU0:Jun 15 12:18:50.521 : SSHD_[65775]: Exchanging versions
RP/0/RP1/CPU0:Jun 15 12:18:50.539 : SSHD_[65775]: Remote protocol version 2.0,
  remote software version Sun_SSH_1.1
RP/0/RP1/CPU0:Jun 15 12:18:50.540 : SSHD_[65775]: In Key exchange
RP/0/RP1/CPU0:Jun 15 12:18:51.137 : SSHD_[65775]: Received ———————> KEXINIT
RP/0/RP1/CPU0:Jun 15 12:18:51.137 : SSHD_[65775]: Calling Receive kexinit 10
RP/0/RP1/CPU0:Jun 15 12:18:51.137 : SSHD_[65775]: Peer Proposal : diffie-hellman-
  group-exchange-sha1,diffie-hellman-group1-sha1
```

```
RP/0/RP1/CPU0:Jun 15 12:18:51.138 : SSHD_[65775]: Peer Proposal : ssh-rsa,ssh-dss
RP/0/RP1/CPU0:Jun 15 12:18:51.139 : SSHD_[65775]: Peer Proposal : aes128-
  ctr,aes128-cbc,arcfour,3des-cbc,blowfish-cbc
RP/0/RP1/CPU0:Jun 15 12:18:51.139 : SSHD_[65775]: Peer Proposal : aes128-
  ctr,aes128-cbc,arcfour,3des-cbc,blowfish-cbc
RP/0/RP1/CPU0:Jun 15 12:18:51.140 : SSHD_[65775]: Peer Proposal : hmac-md5,hmac-
  sha1,hmac-sha1-96,hmac-md5-96
RP/0/RP1/CPU0:Jun 15 12:18:51.140 : SSHD_[65775]: Peer Proposal : hmac-md5,hmac-
  sha1,hmac-sha1-96,hmac-md5-96
RP/0/RP1/CPU0:Jun 15 12:18:51.141 : SSHD_[65775]: Peer Proposal : none,zlib
RP/0/RP1/CPU0:Jun 15 12:18:51.141 : SSHD_[65775]: Peer Proposal : none,zlib
RP/0/RP1/CPU0:Jun 15 12:18:51.141 : SSHD_[65775]: Peer Proposal : i-default
RP/0/RP1/CPU0:Jun 15 12:18:51.141 : SSHD_[65775]: Peer Proposal : i-default
RP/0/RP1/CPU0:Jun 15 12:18:51.164 : SSHD_[65775]: Negotiated Alg : diffie-hellman-
  group1-sha1
RP/0/RP1/CPU0:Jun 15 12:18:51.168 : SSHD_[65775]: Publikey Alg = ssh-dss
RP/0/RP1/CPU0:Jun 15 12:18:51.173 : SSHD_[65775]: Incoming cipher = 3des-cbc
RP/0/RP1/CPU0:Jun 15 12:18:51.176 : SSHD_[65775]: Outgoing cipher = 3des-cbc
RP/0/RP1/CPU0:Jun 15 12:18:51.179 : SSHD_[65775]: Incoming mac = hmac-md5
RP/0/RP1/CPU0:Jun 15 12:18:51.180 : SSHD_[65775]: Outgoing mac = hmac-md5
RP/0/RP1/CPU0:Jun 15 12:18:51.181 : SSHD_[65775]: Keylen Reqd  = 24
RP/0/RP1/CPU0:Jun 15 12:18:51.204 : SSHD_[65775]: Waiting for KEXDH_INIT
RP/0/RP1/CPU0:Jun 15 12:18:51.215 : SSHD_[65775]: Received KEXDH_INIT
RP/0/RP1/CPU0:Jun 15 12:18:51.269 : SSHD_[65775]: Extracting pubkey from crypto
  engine
RP/0/RP1/CPU0:Jun  15 12:18:51.284 :  SSHD_[65775]: Received pubkey from crypto engine
RP/0/RP1/CPU0:Jun 15 12:18:51.285 : SSHD_[65775]: bloblen = 433
RP/0/RP1/CPU0:Jun 15 12:18:51.285 : SSHD_[65775]: prime = 129, subprime = 21, base
  = 128, y =128
RP/0/RP1/CPU0:Jun 15 12:18:51.286 : SSHD_[65775]: Calculating kex hash with
  client_str = SSH-2.0-Sun_SSH_1.1  (len = 19)
RP/0/RP1/CPU0:Jun 15 12:18:51.286 : SSHD_[65775]: server_str = SSH-1.99-Cisco-2.0
  (len = 18)
RP/0/RP1/CPU0:Jun 15 12:18:51.325 : SSHD_[65775]: Sending KEXDH_REPLY
RP/0/RP1/CPU0:Jun 15 12:18:51.328 : SSHD_[65775]: Sending NEWKEYS
RP/0/RP1/CPU0:Jun 15 12:18:51.329 : SSHD_[65775]: Waiting for NEWKEYS
RP/0/RP1/CPU0:Jun 15 12:18:51.362 : SSHD_[65775]: In Authenticate
RP/0/RP1/CPU0:Jun 15 12:18:51.373 : SSHD_[65775]: Request service name - ssh-
  userauth
RP/0/RP1/CPU0:Jun 15 12:18:51.375 : SSHD_[65775]: Sending Servie Accept msg
RP/0/RP1/CPU0:Jun 15 12:18:51.377 : SSHD_[65775]: Waiting for Userauth req
RP/0/RP1/CPU0:Jun 15 12:18:51.391 : SSHD_[65775]: In Interactive shell
RP/0/RP1/CPU0:Jun 15 12:18:51.402 : SSHD_[65775]: Remote channel type - session,
  remote chan id = 0
RP/0/RP1/CPU0:Jun 15 12:18:51.405 : SSHD_[65775]: Winsize = 65536, maxpacksize =
  16384
RP/0/RP1/CPU0:Jun 15 12:18:51.406 : SSHD_[65775]: Sending Channel open success msg
RP/0/RP1/CPU0:Jun 15 12:18:51.437 : SSHD_[65775]: Connecting to VTY Server
```

```
RP/0/RP1/CPU0:Jun 15 12:18:51.494 : SSHD_[65775]: Opening file /dev/vty9999
RP/0/RP1/CPU0:Jun 15 12:18:51.496 : SSHD_[65775]: Allocated pty vty1.
RP/0/RP1/CPU0:Jun 15 12:18:51.497 : SSHD_[65775]: Setting window size row = 24,
  col = 106
RP/0/RP1/CPU0:Jun 15 12:18:51.615 : SSHD_[65775]: Spawned shell
RP/0/RP1/CPU0:Jun 15 12:18:51.677 : SSHD_[65775]: event_contex_init done
!
! Show command to verify the SSH session detail on the router.
!
RP/0/RP1/CPU0:CRS1-1#show ssh session details
SSH version : Cisco-2.0
id  key-exchange  pubkey  incipher  outcipher  inmac   outmac
-----------------------------------------------------------------
Incoming Session
diffie-hellman  ssh-dss  3des-cbc  3des-cbc  hmac-md5  hmac-md5
! A command output showing the incoming SSH TCP session
!
RP/0/RP1/CPU0:CRS1-1#show tcp brief
   PCB      VRF-ID      Recv-Q Send-Q Local Address      Foreign Address      State
0x482e2c30 0x60000000      0      0  :::22              :::0                 LISTEN
0x482e2ea0 0x60000001      0      0  :::22              :::0                 LISTEN
0x482e8248 0x00000000      0      0  :::22              :::0                 LISTEN
0x482e5a38 0x60000000      0      0  10.0.0.11:646      10.0.0.31:35777      ESTAB
0x482cc0a8 0x60000000      0      0  10.0.0.11:646      10.0.0.21:57878      ESTAB
0x482deff4 0x60000000      0      0  10.10.20.31:23     10.10.20.100:61512   ESTAB
0x482e7714 0x60000000      0      0  10.10.20.31:22     10.10.20.100:61532   ESTAB
0x482e8380 0x60000000      0      0  0.0.0.0:22         0.0.0.0:0            LISTEN
0x482e2d68 0x60000001      0      0  0.0.0.0:22         0.0.0.0:0            LISTEN
0x482e8598 0x00000000      0      0  0.0.0.0:22         0.0.0.0:0            LISTEN
0x482d0660 0x60000000      0      0  0.0.0.0:23         0.0.0.0:0            LISTEN
0x482e0dc4 0x00000000      0      0  0.0.0.0:23         0.0.0.0:0            LISTEN
0x482cf2e4 0x60000000      0      0  0.0.0.0:639        0.0.0.0:0            LISTEN
0x482cd9e4 0x60000000      0      0  0.0.0.0:646        0.0.0.0:0            LISTEN
```

Example 6-11 shows an SSH session created from a UNIX host to the router and the corresponding debug output produced on the console. The debug output shows the exchanging of SSH version between the UNIX host and the router as well as the negotiation of the Diffie-Hellman key exchange. The example also presents the **show ssh session detail** command's output showing the details of the SSH session. The output of **show tcp brief** shows the TCP port 22 sessions that identifies the incoming SSH connection.

Management Plane Protection

Management plane refers to a router's architectural components involved in the processing of traffic that is meant for the management of the routing platform. Management Plane Protection (MPP) is a relatively new feature in IOS XR; it was introduced in Release 3.5.0. It helps control the interfaces on which network management traffic can enter the router. The capability helps enhance the router-level security and allows the network administrator better granularity in controlling management access to the router.

Following are the salient features of MPP:

- Enhances the manageability and security aspects of IOS XR.
- Helps alleviate the need to configure more access lists in controlling router access.
- Management ports on RP and DRP are not configurable under MPP because they are out of band by default.
- Controls incoming traffic for protocols, such as TFTP, Telnet, Simple Network Management Protocol (SNMP), SSH, and HTTP.
- Allows control for both in-band and out-of-band interfaces.
- Can specify a peer IPv4 or IPv6 address or subnet from which traffic is allowed, thus providing more control.

In the context of MPP, an *in-band* management interface is an interface that receives and processes management packets as well as forwards Internet traffic. This interface may also be referred to as a *shared management interface*. An out-of-band interface allows only management protocol traffic to be forwarded or processed. This type of interface does not process or receive any customer or Internet traffic and, therefore, has lower potential for becoming a victim of a DoS attack. Out-of-band interfaces are usually also the last hop interfaces in the life of a packet, and these packets are then processed by higher-layer protocols on the router.

Example 6-12 illustrates the configuration steps for MPP.

Example 6-12 *Configuring MPP*

```
RP/0/RP1/CPU0:CRS1-1#configure t
RP/0/RP1/CPU0:CRS1-1(config)#control-plane
RP/0/RP1/CPU0:CRS1-1(config-ctrl)#management-plane
RP/0/RP1/CPU0:CRS1-1(config-mpp)#inband
RP/0/RP1/CPU0:CRS1-1(config-mpp-inband)#interface tenGigE 0/0/0/0
RP/0/RP1/CPU0:CRS1-(config-mpp-inband-TenGigE0_0_0_0)#allow telnet
```

```
RP/0/RP1/CPU0:CRS1-(config-mpp-inband-TenGigE0_0_0_0)#commit
RP/0/RP1/CPU0:CRS1-(config-mpp-inband-TenGigE0_0_0_0)#exit
RP/0/RP1/CPU0:CRS1-1(config-mpp-inband)#exit
RP/0/RP1/CPU0:CRS1-1(config-mpp)#out-of-band
RP/0/RP1/CPU0:CRS1-1(config-mpp-outband)#vrf red
RP/0/RP1/CPU0:CRS1-1(config-mpp-outband)#interface tenGigE 0/0/0/0.1
RP/0/RP1/CPU0:CR(config-mpp-outband-TenGigE0_0_0_0.1)#allow snmp
RP/0/RP1/CPU0:CR(config-mpp-outband-TenGigE0_0_0_0.1)#allow telnet
RP/0/RP1/CPU0:CR(config-mpp-outband-TenGigE0_0_0_0.1)#commit
RP/0/RP1/CPU0:CR(config-mpp-outband-TenGigE0_0_0_0.1)#
! Using an MPP show command
RP/0/RP1/CPU0:CRS1-1#show mgmt-plane
Management Plane Protection
inband interfaces
————————————
interface - TenGigE0_0_0_0
        telnet configured -
                All peers allowed
outband interfaces
————————————
interface - TenGigE0_0_0_0.1
        telnet configured -
                All peers allowed
        snmp configured -
                All peers allowed
RP/0/RP1/CPU0:CRS1-1#
```

Example 6-12 shows MPP configuration where the Telnet protocol is enabled for only one in-band interface (Tengig0/0/0/0), and the out-of-band management interface Tengig0/0/0/0.1 under vrf red is enabled for telnet and SNMP.

Securing the Forwarding Plane

Forwarding plane refers to a router's forwarding path involved in processing transit traffic or in processing traffic that is destined to the router. The traffic destined to the router is also sometimes termed *for_us* traffic. The forwarding plane constitutes the packet-forwarding, switching, and queuing components involved in the packet flow. This section introduces various forwarding plane features and provides configuration examples of each. The main features covered in forwarding plane security are ACLs, Unicast Reverse Path Forwarding (uRPF), and Local Packet Transport Services (LPTS).

Access Control Lists

ACL filtering allows the network administrator to control packet flow through the network. Such control helps limit undesirable network traffic and helps restrict network use by certain users or devices. ACLs provide the ability to permit or deny packets from passing through specific router interfaces. Access lists also find several uses in providing granularity and control to control plane protocols.

Following are some of the key features of IOS XR access lists:

- **Named access lists:** Cisco IOS XR uses named access lists only. Internally, the access list is treated as a string or name. IOS XR uses only named access lists. Even if a number is used to denote an access list, it is internally treated as a string or a name.
- **Standard or Extended Keywords:** IOS XR does not use standard and extended keywords in specifying an access list. An access list can include mixed Access Control Elements (ACE) that use only source-based filtering or both source- and destination-based filtering that may be combined with protocol port operations.
- **Locally originated traffic:** Cisco IOS XR egress ACLs do not filter traffic originated by the router.
- **ACL numbering and resequence:** Cisco IOS XR ACLs use line numbering to help replace a particular line in an ACL definition. An option is provided to resequence the ACL line numberings if required.
- **Remarks:** Cisco IOS XR ACLs provide the ability to insert remarks in an access list to help explain the purpose of the particular line in an ACL.
- **Log messages:** Cisco IOS XR provides the ability to log an ACL. Logging an ACL produces a syslog message when a packet matches a line with the **log** keyword. This operation is CPU intensive and must not be enabled for high speed traffic rates. Usually an ACL with a **log** keyword can be used for ACLs applied to vty lines. A **log** keyword may also be used for temporary debugging purposes, keeping in mind that its use is CPU intensive.
- **ICMP unreachables:** IOS XR ACL deny packet operation on an interface produces a rate-controlled ICMP unreachable message. This ICMP message can be disabled from the interface by using the CLI **no ipv4 unreachables**.

Example 6-13 shows the creation of an access list that has the following properties:

- ACL with name CRS-Core.
- Permits incoming LDP and BGP sessions from the peer address 67.13.1.1 destined to 67.13.2.1.
- The ACL permits any traffic destined to TCP ports 80 and 8080.
- The ACL permits SSH traffic from host 62.133.1.1.
- The rest of the traffic is denied.

Example 6-13 *Configuring an ACL Named CRS-Core*

```
RP/0/RP1/CPU0:CRS1-1(config)#ipv4 access-list CRS-Core
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp host 67.13.1.1 eq ldp host
  67.13.2.1
```

```
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp host 67.13.1.1 host 67.13.2.1 eq
  ldp
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp host 67.13.1.1 host 67.13.2.1 eq
  bgp
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp any eq 80 any
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp any any eq 80
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp any eq 8080 any
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp any any eq 8080
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit tcp host 62.133.1.1 any eq 22
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit icmp 65.10.20.0 0.0.0.255 any echo
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#permit icmp 65.10.20.0 0.0.0.255 any echo-
  reply
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#commit
RP/0/RP1/CPU0:CRS1-1(config-ipv4-acl)#exit
RP/0/RP1/CPU0:CRS1-1(config)#
```

Example 6-14 shows the application of the access list ingress on the interface tenGigE 0/0/0/0.

Example 6-14 *Applying ACL Named CRS-Core*

```
RP/0/RP1/CPU0:CRS1-1#show access-lists ipv4 CRS-Core
ipv4 access-list CRS-Core
 10 permit tcp host 67.13.1.1 eq ldp host 67.13.2.1
 20 permit tcp host 67.13.1.1 host 67.13.2.1 eq ldp
 30 permit tcp host 67.13.1.1 host 67.13.2.1 eq bgp
 40 permit tcp any eq www any
 50 permit tcp any any eq www
 60 permit tcp any eq 8080 any
 70 permit tcp any any eq 8080
 80 permit tcp host 62.133.1.1 any eq 22
 90 permit icmp 65.10.20.0 0.0.0.255 any echo
 91 permit icmp 65.10.20.0 0.0.0.255 any echo-reply

! Applying the access-list to an interface
RP/0/RP1/CPU0:CRS1-1#configure t
RP/0/RP1/CPU0:CRS1-1(config)#interface tenGigE 0/0/0/1
RP/0/RP1/CPU0:CRS1-1(config-if)#ipv4 access-group CRS-Core ingress
RP/0/RP1/CPU0:CRS1-1(config-if)#commit
```

Example 6-15 shows the access list created in Example 6-14 from the hardware perspective of the node to which it is applied. An access list applied to the forwarding path may be queried using the hardware keyword to ensure that the configuration has been accepted by the linecard hardware.

Example 6-15 *Access List in Hardware*

```
RP/0/RP1/CPU0:CRS1-1#show access-lists ipv4 CRS-Core hardware ingress location
  0/0/cpu0
ipv4 access-list CRS-Core
 10 permit tcp host 67.13.1.1 eq ldp host 67.13.2.1
 20 permit tcp host 67.13.1.1 host 67.13.2.1 eq ldp
 30 permit tcp host 67.13.1.1 host 67.13.2.1 eq bgp
 40 permit tcp any eq www any
 50 permit tcp any any eq www
 60 permit tcp any eq 8080 any
 70 permit tcp any any eq 8080
 80 permit tcp host 62.133.1.1 any eq 22
 90 permit icmp 65.10.20.0 0.0.0.255 any echo
 91 permit icmp 65.10.20.0 0.0.0.255 any echo-reply
```

Table 6-2 lists the key **show** and **debug** commands related to access lists.

Table 6-2 *Key ACL Operations and debug Commands*

Command	Description
show access-lists afi-all	Shows configured access lists for IPv4 and IPv6 address families.
show access-lists maximum [*detail* | *<cr>*]	Shows the maximum configurable and current configured number of ACLs.
show access-lists usage pfilter location *line_card_location*	Indicates which access lists are applied to the node and whether they are applied ingress or egress.
show access-lists hardware {*ingress* | *egress*} **location** *line_card_location*	Shows ACL information as applied to line card hardware.
debug pfilter-ea errors location *line_card_location*	Debugs any errors encountered when applying ACL. Should be used only if there is a problem with applying an ACL.

Unicast RPF

Unicast Reverse Path Forwarding (uRPF) is another useful IOS XR feature that helps prevent malicious traffic from entering a service provider network. uRPF may be used in strict and loose modes. Enabling strict uRPF on an interface helps the forwarding path analyze the incoming traffic's source address. If the reverse path back to the source address of incoming packet is not learned via the interface on which strict uRPF is enabled, the packet is dropped. Loose uRPF is useful when a case of asymmetric routing might be present on the network. In the case of loose uRPF, the route for the source interface must be in the routing table. Configuration options may also allow default routes to satisfy loose uRPF requirements.

The following command configures strict or loose uRPF at the interface level:

```
{ipv4 ¦ ipv6} verify unicast source reachable-via {any ¦ rx} [allow-default]
  [allow-self-ping]
```

The explanation of this command follows:

- Using the **any** option after **verify unicast source reachable-via** enables loose uRPF.
- Using the **rx** option after **verify unicast source reachable-via** enables strict uRPF.
- The **allow-default** option allows uRPF check to be true against a default route. This option is equally applicable to loose and strict uRPF.
- The **allow-self-ping** option allows the router to ping itself and is applicable to both loose and strict uRPF.

Example 6-16 shows the enabling of strict uRPF on a CRS interface and depicts a CEF command to check whether the configuration has been enforced.

Example 6-16 *Strict uRPF on the tenGigE Interface*

```
RP/0/RP1/CPU0:CRS1-1(config)#interface tenGigE 0/0/0/1
RP/0/RP1/CPU0:CRS1-1(config-if)#ipv4 verify unicast source reachable-via rx
RP/0/RP1/CPU0:CRS1-1(config-if)#commit
!
! The following show command shows if the feature has been enabled
RP/0/RP1/CPU0:CRS1-1#show cef ipv4 interface tenGigE 0/0/0/1
TenGigE0/0/0/1 is up (if_handle 0x01080040)
  Interface last modified Jan 12 22:54:42, modify
  Reference count 2
  Forwarding is enabled
  ICMP redirects are never sent
  IP MTU 1500, TableId 0xe0000000
  IP unicast RPF check is enabled
  RPF mode strict
  Protocol Reference count 2
  Primary IPV4 local address 65.10.20.2/32
```

Example 6-17 shows the strict uRPF in action. The router does not have a route to a source of traffic that comes from IP address 171.1.1.1; on receiving the traffic, the strict uRPF feature drops this traffic. Example 6-17 depicts a CEF-related show command for determining uRPF drop statistics.

Example 6-17 *Strict uRPF on the tenGigE Interface*

```
RP/0/RP1/CPU0:CRS1-1#show route 171.1.1.1
% Network not in table
!
```

```
! shows RPF statistics
RP/0/RP1/CPU0:CRS1-1#show cef ipv4 interface tenGigE 0/0/0/1 rpf-statistics
Unicast RPF drops 1000
```

Local Packet Transport Service

The forwarding plane security section has so far discussed features such as ACLs and uRPF, which filter packets based on certain criteria. This section discusses Local Packet Transport Service (LPTS). LPTS provides software architecture to deliver locally destined traffic to the correct node on the router and provides security against overwhelming the router resources with excessive traffic. LPTS achieves security by policing flows of locally destined traffic to a value that can be easily sustained by the CPU capabilities of the platform.

The first question you might ask is what sort of traffic constitutes locally destined traffic. Although routers are in the business of forwarding packets, there are scenarios in which the traffic may be locally destined, including the following:

- All IPv4, IPv6, and MPLS traffic related to routing protocols, or control plane such as MPLS LDP or RSVP. The control plane computations for protocols are done on the Router Processor (RP) of the router. Therefore, whenever routing or MPLS control plane traffic is received on a line card interface, it needs to be delivered to the RP of the router.
- MPLS packets with the Router Alert label
- IPv4, IPv6, or MPLS packets with a TTL less than 2
- IPv4 or IPv6 packets with options
- IP packets requiring fragmentation or reassembly
- Layer 2 keepalives
- Address Resolution Protocol (ARP) packets
- ICMP message generation and response

Table 6-3 lists the various types of locally destined traffic and indicates the router's node on which the traffic may be processed.

Table 6-3 *CRS-1 Release 3.6.0 for_us Packet Processing*

Received Traffic Type	Processed in Packet Switching Engine	Processed by Line Card CPU	Processed by Route Processor
Transit Traffic			
Transit Packets	Undergoes configured features (ACL, QoS, and so on)	-	-

Received Traffic Type	**Processed in Packet Switching Engine**	**Processed by Line Card CPU**	**Processed by Route Processor**
Transit Packets, IP Options	LPTS Policed	X	-
Transit Packets, IP Option "Router Alert"	LPTS Policed	X	X
Packets failed BGP TTL Security Hack (BTSH) and Generalized TTL Security Management (GTSM)	BTSH/GTSM	-	-
Packets that require ARP resolution	LPTS Policed	X	-
Unicast Receive Traffic			
ICMP echo request, packets requiring logging	LPTS Policed	X	-
Any other ICMP (also ICMP with options)	LPTS Policed	X	-
Management traffic (SSH, SNMP, XML, and so on)	LPTS Policed	-	X
Management traffic (Netflow, CDP)	LPTS Policed	X	-
Routing (BGP, OSPF, ISIS, and so on)	LPTS Policed	-	X
Multicast, Broadcast			
Multicast control traffic (OSPF, PIM, HSRP, and so on)	LPTS Policed	-	X
First packet of multicast stream	LPTS Policed	X	-
Broadcasts	LPTS Policed	X	X
Special Cases			
Traffic needing fragmentation	LPTS Policed	X	-
MPLS traffic needing fragmentation	LPTS Policed	X	-
L2 packets (keepalives and so on)	LPTS Policed	X	-

LPTS provides sort of a built-in firewall for an IOS XR router by taking preemptive measures for traffic flows destined to the router. The forthcoming discussions explain how LPTS provides its protection mechanisms.

Mechanics Behind LPTS: A High-Level Overview

Cisco IOS XR runs on platforms with a distributed architecture. Distributed architecture implies that the control plane and the forwarding planes are decoupled for meeting higher routing and forwarding performance objectives. As Table 6-3 in the preceding section shows, an IOS XR router might need to deliver different types of for_us packets to different nodes within the router. Additionally, IOS XR supports process placement on CRS-1 platforms using Distributed Route Processors (DRP). Therefore, a line card receiving a control plane packet needs to make complex decisions regarding the node to which a packet might need to be delivered, keeping in mind that the router may be using a DRP for distributing a control plane process. Furthermore, nonstop routing (NSR) features might require a control packet be replicated both to an active and a standby RP.

Figure 6-3 provides a high-level overview of LPTS.

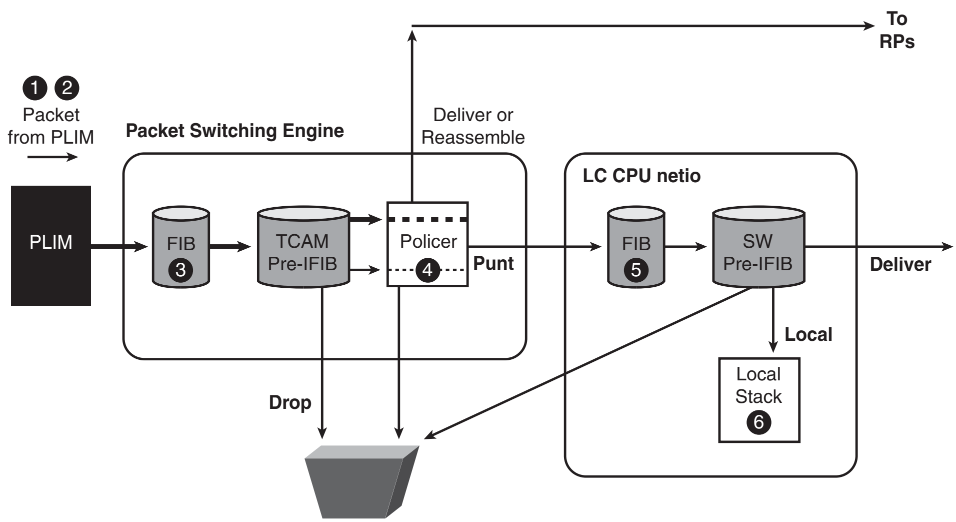

Figure 6-3 *Local Packet Transport Service*

The process follows:

1. On a CRS-1 router, the Physical layer Interface Module (PLIM) receives the frame.
2. On receiving the packet and performing the necessary layer 1 and 2 checks, the PLIM extracts the layer 3 packet and passes it to the forwarding ASIC or the *Packet Switching Engine (PSE)* as it is commonly called.
3. The L3 forwarding engine does a Forwarding Information Base (FIB) lookup and determines whether the packet is a locally destined for_us packet.
4. The LPTS infrastructure maintains tables in the line card's TCAM and also on the RP for handling the for_us packets. The table on the RP is a detailed list of all possible flows of traffic types that can be destined to the router. The detailed table on RP is called the *IFIB*. A smaller table that is a subset of IFIB exists on the line card and this table is referred to as the *pIFIB*. The pIFIB lists flows of critical traffic. These tables are populated by a set of processes known as a LPTS Port Arbitrator (lpts_pa) and LPTS flow manager (lpts_fm). A process called pifibm_server runs on the line card and is responsible for programming hardware for the policing values for different flows. To qualify for a match in the pIFIB, the incoming packet must exactly match the pIFIB table entry in a single lookup.
5. Consider a packet that arrives on a line card and a pIFIB lookup returns a full match. The packet then gets assigned a Fabric Group Identifier (FGID) allocated by the lpts_pa process. FGID serves as an identifier that helps a packet traverse the path through the various ASICs on the switch fabric to be delivered to FabricQ asic on the destination node from where the packet finds its way to the primary/standby RP, DRP, or the line card CPU. The destination node could also be an RP, a DRP, or the line card CPU of the line card on which the packet was received. In case a line card pIFIB entry results in a partial match the incoming packet is referred to the IFIB maintained on the RP.
6. The CPU on the RP, DRP, and line card run the software processes that decapsulate the packet and deliver them to the correct stack.

The discussion related to Figure 6-3 gives a simplified overview of LPTS mostly from the point of view of local packet delivery. However, a key feature of LPTS includes policing the locally destined flows to values deemed safe for CPU resources.

Consider Example 6-18, which shows the LPTS entries accompanying a BGP configuration.

Example 6-18 *BGP Entries in LPTS*

```
! show command indicating the committed BGP configuration
!
RP/0/RP1/CPU0:CRS1-1#show running-config router bgp
router bgp 102
 bgp router-id 192.168.254.1
```

```
 address-family ipv4 unicast
 !
 neighbor 65.10.20.1
  remote-as 101
  address-family ipv4 unicast
  !
 !
!
!
! Following show command shows the entries created in IFIB
RP/0/RP1/CPU0:CRS1-1#show lpts ifib brief ¦ include BGP
 BGP4      default  65.10.20.2.179 65.10.20.1.45  TCP    any           0/RP1/CPU0
 BGP4      default  any.179 65.10.20.1            TCP    any           0/RP1/CPU0
! Following show command shows entries in PIFIB.
! The output of the following show command is usually quite large and is
! modified to show only BGP entries in LPTS PIFIB
RP/0/RP1/CPU0:CRS1-1#show lpts pifib brief
RP/0/RP1/CPU0:CRS1-1#show lpts pifib brief
* - Any VRF; I - Local Interest;
X - Drop; R - Reassemble;
 Type        VRF-ID   Local, Remote Address.Port L4    Interface    Deliver
 ————— ———— —————————————— ——. ——————— ———————.
 ISIS        *         - -                       -     any          0/RP1/CPU0
 IPv4_frag   *        any any                    any   any          R
 IPv4        default  224.0.0.1 any              IGMP  Lo0          0/RP1/CPU0
 IPv4        default  224.0.0.2 any              IGMP  Lo0          0/RP1/CPU0
 IPv4        default  224.0.0.22 any             IGMP  Lo0          0/RP1/CPU0
 IPv4        default  any any                    IGMP  Lo0          0/RP1/CPU0
 IPv4        default  224.0.1.40.496 any         UDP   Lo0          0/RP1/CPU0
 IPv4        default  224.0.0.13 any             103   Lo0          [11295]
 IPv4        default  224.0.0.1 any              IGMP  Lo1          0/RP1/CPU0
 IPv4        default  224.0.0.2 any              IGMP  Lo1          0/RP1/CPU0
 IPv4        default  224.0.0.22 any             IGMP  Lo1          0/RP1/CPU0
 IPv4        default  any any                    IGMP  Lo1          0/RP1/CPU0
 IPv4        default  224.0.0.13 any             103   Lo1          [11295]
 IPv4        default  224.0.0.1 any              IGMP  Lo100        0/RP1/CPU0
 IPv4        default  224.0.0.2 any              IGMP  Lo100        0/RP1/CPU0
 IPv4        default  224.0.0.22 any             IGMP  Lo100        0/RP1/CPU0
 IPv4        default  any any                    IGMP  Lo100        0/RP1/CPU0
 IPv4        default  224.0.0.13 any             103   Lo100        [11295]
 IPv4        default  224.0.0.1 any              IGMP  Lo101        0/RP1/CPU0
 IPv4        default  224.0.0.2 any              IGMP  Lo101        0/RP1/CPU0
 IPv4        default  224.0.0.22 any             IGMP  Lo101        0/RP1/CPU0
 IPv4        default  any any                    IGMP  Lo101        0/RP1/CPU0
 IPv4        default  224.0.0.13 any             103   Lo101        [11295]
```

```
IPv4       default  224.0.0.1 any           IGMP  Lo10           0/RP1/CPU0
IPv4       default  224.0.0.2 any           IGMP  Lo10           0/RP1/CPU0
IPv4       default  224.0.0.22 any          IGMP  Lo10           0/RP1/CPU0
IPv4       default  any any                 IGMP  Lo10           0/RP1/CPU0
IPv4       default  224.0.0.13 any          103   Lo10           [11295]
IPv4       default  any.23 any              TCP   Mg0/RP1/CPU0/0 0/RP1/CPU0
IPv4       default  any.161 any             UDP   Mg0/RP1/CPU0/0 0/RP1/CPU0
IPv4       default  any.639 1.1.1.1         TCP   any            0/RP1/CPU0
IPv4       default  10.0.0.11.646 10.0.0.21.57 TCP any           0/RP1/CPU0
IPv4       default  10.0.0.11.646 10.0.0.31.35 TCP any           0/RP1/CPU0
IPv4       default  10.10.20.31.23 10.10.20.10 TCP any           0/RP1/CPU0
IPv4       default  65.10.20.2.179 65.10.20.1. TCP any           0/RP1/CPU0
IPv4       default  any.179 65.10.20.1      TCP   any            0/RP1/CPU0
IPv4       default  any.646 any             UDP   any            0/RP1/CPU0
IPv4       default  any.3232 any            UDP   any            [11295]
IPv4       default  any.3503 any            UDP   any            0/RP1/CPU0
IPv4       default  any.50051 any           UDP   any            0/RP1/CPU0
IPv4       default  any.50052 any           UDP   any            0/RP1/CPU0
IPv4       default  any.50053 any           UDP   any            0/RP1/CPU0
IPv4       default  any.50054 any           UDP   any            0/RP1/CPU0
IPv4       default  any any                 103   any            [11295]
IPv4       default  any any                 115   any            0/RP1/CPU0
IPv4       default  any any                 255   any            0/RP1/CPU0
IPv4       *         any.ECHO any           ICMP  any            XI
IPv4       *         any.TSTAMP any         ICMP  any            XI
IPv4       *         any.MASKREQ any        ICMP  any            XI
IPv4       *         any any.179            TCP   any            0/RP1/CPU0
IPv4       *         any.179 any            TCP   any            0/RP1/CPU0
IPv4       *         any any                TCP   any            0/RP1/CPU0
IPv4       *         any any                UDP   any            0/RP1/CPU0
IPv4       *         224.0.0.5 any          OSPF  any            0/RP1/CPU0
IPv4       *         224.0.0.6 any          OSPF  any            0/RP1/CPU0
IPv4       *         any any                OSPF  any            0/RP1/CPU0
IPv4       *         any any                any   any            0/RP1/CPU0
IPv6_frag  *        any any                 any   any            R
IPv6       *         any any.179            TCP   any            0/RP1/CPU0
IPv6       *         any.179 any            TCP   any            0/RP1/CPU0
IPv6       *         any any                TCP   any            0/RP1/CPU0
IPv6       *         any any                UDP   any            0/RP1/CPU0
IPv6       *         any.ECHOREQ any        ICMP6 any            XI
IPv6       *         any.NDRTRSLCT any      ICMP6 any            XI
IPv6       *         any.NDRTRADV any       ICMP6 any            XI
IPv6       *         any.NDNBRSLCT any      ICMP6 any            XI
IPv6       *         any.NDNBRADV any       ICMP6 any            XI
IPv6       *         any.NDREDIRECT any     ICMP6 any            XI
```

```
 IPv6       *        ff02::5 any              OSPF  any            0/RP1/CPU0
 IPv6       *        ff02::6 any              OSPF  any            0/RP1/CPU0
 IPv6       *        any any                  OSPF  any            0/RP1/CPU0
 IPv6       *        any any                  any   any            0/RP1/CPU0
RP/0/RP1/CPU0:CRS1-1#! Hardware Policing values in pifib
!
RP/0/RP1/CPU0:CRS1-1#show lpts pifib hardware police location 0/0/cpu0
-------------------------------------------------------------
                 Node 0/0/CPU0:
-------------------------------------------------------------
 Burst = 100ms for all flow types
-------------------------------------------------------------
FlowType                 Policer  Type      Cur. Rate  Def. Rate  Accepted  Dropped
----------------------   -------  -------   ---------  ---------  --------  -------
unconfigured-default     100      Static    500        500        0         0
Fragment                 106      Static    1000       1000       0         0
OSPF-mc-known            107      Static    20000      20000      248647    0
OSPF-mc-default          111      Static    5000       5000       43431     0
OSPF-uc-known            161      Static    5000       5000       0         0
OSPF-uc-default          162      Static    1000       1000       0         0
ISIS-known               108      Static    20000      20000      536237    0
ISIS-default             112      Static    5000       5000       4         0
BGP-known                113      Static    25000      25000      41        0
BGP-cfg-peer             114      Static    10000      10000      5         0
BGP-default              115      Static    10000      10000      54        0
PIM-mcast                116      Static    23000      23000      0         0
PIM-ucast                117      Static    10000      10000      0         0
IGMP                     118      Static    3500       3500       0         0
ICMP-local               119      Static    2500       2500       20        0
ICMP-app                 120      Static    2500       2500       0         0
na                       164      Static    2500       2500       0         0
ICMP-default             121      Static    2500       2500        0        0
LDP-TCP-known            122      Static    25000      25000      290       0
LDP-TCP-cfg-peer         152      Static    10000      10000      0         0
LDP-TCP-default          154      Static    10000      10000      0         0
LDP-UDP                  158      Static    2500       2500       519490    0
All-routers              160      Static    10000      10000      0         0
LMP-TCP-known            123      Static    25000      25000      0         0
LMP-TCP-cfg-peer         153      Static    10000      10000      0         0
LMP-TCP-default          155      Static    10000      10000      0         0
LMP-UDP                  159      Static    2500       2500       0         0
RSVP-UDP                 124      Static    7000       7000       0         0
RSVP                     125      Static    7000       7000       0         0
IKE                      126      Static    1000       1000       0         0
IPSEC-known              128      Static    3000       3000       0         0
```

```
IPSEC-default          127    Static   1000     1000     0      0
MSDP-known             129    Static   1000     1000     0      0
MSDP-cfg-peer          130    Static   1000     1000     0      0
MSDP-default           131    Static   1000     1000     0      0
SNMP                   132    Static   2000     2000     0      0
NTP                    133    Static   500      500      0      0
SSH-known              134    Static   1000     1000     0      0
SSH-default            135    Static   1000     1000     0      0
HTTP-known             137    Static   1000     1000     0      0
HTTP-default           138    Static   1000     1000     0      0
SHTTP-known            139    Static   1000     1000     0      0
IFIB_FT_SHTTP_DEFAULT  140    Static   1000     1000     0      0
TELNET-known           141    Static   1000     1000     0      0
TELNET-default         142    Static   1000     1000     0      0
CSS-known              143    Static   1000     1000     0      0
CSS-default            144    Static   1000     1000     0      0
RSH-known              145    Static   1000     1000     0      0
RSH-default            146    Static   1000     1000     0      0
UDP-known              147    Static   25000    25000    0      0
UDP-listen             156    Static   4000     4000     0      0
UDP-cfg-peer           157    Static   4000     4000     0      0
UDP-default            101    Static   500      500      69     0
TCP-known              148    Static   25000    25000    0      0
TCP-listen             149    Static   25000    25000    0      0
TCP-cfg-peer           150    Static   25000    25000    0      0
TCP-default            102    Static   500      500      60     0
Mcast-known            151    Static   25000    25000    0      0
Mcast-default          103    Static   500      500      0      0
Raw-listen             104    Static   500      500      0      0
Raw-default            105    Static   500      500      0      0
Ip-Sla                 163    Static   10000    10000    0      0
EIGRP                  109    Static   20000    20000    0      0
RIP                    110    Static   20000    20000    0      0
L2TPv3                 165    Static   3000     3000     0      0
na                     166    Static   100      100      0      0
————————————
statistics:
Packets accepted by deleted entries: 1188045
Packets dropped by deleted entries: 0
Run out of statistics counter errors: 0
```

Example 6-18 configures BGP and uses it to demonstrate the LPTS concept. The example creates a BGP process for AS 102 and configures a neighbor 65.10.20.2. On configuring a BGP peer, LPTS creates a flow for the configured peer with TCP port 179. A BGP flow is also created in pIFIB with a destination node of 0/RP1/CPU0 because the BGP routing protocol runs on the RP of the router and the active RP is the destination node for BGP packets.

Example 6-18 shows the policer in line card hardware and shows three different policers for BGP, which exist regardless of BGP configuration. Policer 113 in the example for BGP flow type BGP-known signifies a well established BGP session that actively participates in BGP route advertisement. Policer 114 BGP-cfg-peer represents a new session or recently established session that has not yet elevated to a level of an established session. BGP-default identified by policer 115 represents a default entry for BGP flow. This flow also helps with any latency in hardware programming for new configurations or accounts for a TCP session that might be initiated to port 179 for debugging purposes. The example shows a higher policer rate of 25,000 packets per second (pps) for established sessions compared to 10,000 pps for all other categories of BGP traffic flows.

Configuring LPTS

The LPTS discussion so far has focused on default policers preprogrammed in hardware TCAMs on CRS-1 line cards. Release 3.6 of IOS XR provides the user the ability to configure LPTS policer values. The general syntax for LPTS policer configurations is listed as follows:

lpts pifib hardware police [**location** *node-id*]
flow {*flow_type***} {rate** *rate***}**

The flow rate is in packets per second (pps).

Example 6-19 demonstrates LPTS configuration.

Example 6-19 *Configuring LPTS BGP-default Policer Value to 1000 PPS*

```
RP/0/RP1/CPU0:CRS1-1(config)#lpts pifib hardware police
RP/0/RP1/CPU0:CRS1-1(config-pifib-policer-global)#flow bgp default rate 1000
RP/0/RP1/CPU0:CRS1-1(config-pifib-policer-global)#commit
!
! show command to verify newly configured LPTS policer values
!
RP/0/RP1/CPU0:CRS1-1#show lpts pifib hardware police location 0/0/cpu0 ¦ inc BGP
BGP-known                113      Static   25000       25000       0           0
BGP-cfg-peer             114      Static   10000       10000       0           0
BGP-default              115      Global   1000        10000       237         0
```

Example 6-19 shows a configuration change applied globally to all the line cards in the SDR or logical router to change the policer for BGP-default flow. Alternatively, a configuration may be created for a particular line card location that has the effect of overwriting the global LPTS policing configuration only for the location for which it is created.

Summary

This chapter discussed Cisco IOS XR security aspects. In this chapter we explored the AAA feature and its configuration aspects that are used in managing access to a router running the IOS XR operating system. Although the concepts of AAA are independent of platform and operating system, IOS XR exhibits key characteristics of a large-scale operating system that has unique requirements, such as elaborate access policies. This chapter introduced the IOS XR concepts of predefined users such as root-system, root-lr, netadmin, and cisco-support—each of which has well-defined roles and privileges.

IOS XR's AAA model contains the notion of task permissions for any control, configure, or monitor operation. Tasks are represented as task IDs. A task ID defines the permission to execute an operation for a given user. If the user is associated with a task ID through a user group, that user can execute any of the operations associated with that task ID. All IOS XR CLI are associated with one or more task IDs. Task IDs always imply granted permission and not denied ones. Furthermore, task IDs are always associated with one of the task classes: READ, WRITE, EXECUTE, or DEBUG.

AAA provides transparent use of local, on-the-box authentication as well as remote authentication done with an external TACACS+ or RADIUS server.

This chapter also briefly introduced Secure Shell (SSH), access lists, and uRPF features. This chapter elucidated the concepts behind Local Packet Transport Service (LPTS) in providing an integral firewall for the IOS XR running router.

References

- **Cisco.** Configuring AAA Services on Cisco IOS XR Software. http://www.cisco.com/
- **Cisco.** Implementing Management Plane Protection on Cisco IOS XR Software. http://www.cisco.com/
- **Cisco.** Implementing LPTS on Cisco IOS XR Software. http://www.cisco.com/
- **Cisco.** Implementing Access Lists and Prefix Lists on Cisco IOS XR Software. http://www.cisco.com/

Index

A

AA (Assume Alive), sparse mode forwarding, 370
AAA (Authentication/Authorization/ Accounting)
aaa group server command, 172
accounting, router access, 161
authentication
aaa authentication login chap-6 group chap6 local command, 172
aaa authentication login remote local command, named SDR logins, 395
RADIUS protocol, 172-173
router access, 161
authorization
aaa authorization exec default none command, 172
router access, 161
show aaa task supported command, 162
aborting configuration sessions, 122
ABR (area border routers), OSPF, 212
absolute refpoints, 105-107
Accept A flags, sparse mode forwarding, 370
accounting, router access, 161
ACL (access control lists)
configuring, 179-180
debug pfilter-ea errors location command, 181
extended keywords, 179
filtering, 178-181
ICMP unreachables, 179
keywords, 179
line numbering/resequencing, 179
locally originated traffic, 179
log messages, 179
named access lists, 179
remarks, 179
show access-lists afi-all command, 181
show access-lists hardware location command, 181
show access-lists maximum command, 181
show access-lists usage pfilter location command, 181
activating packages, 126-127
active configurations. *See* running configuration
add rip-metric option, RIP configuration, 198
address families, configuring, 251-252
adjacencies (multiarea), configuring OSPFv2 in, 226-227
admin directory (CFS), 105
admin plane, 100, 161
Admin SysDB Server, 108
ADR (atomic descriptor ring), 34

af-group BGP configuration group, 252-256
affinity (processes), 42-43
AND Boolean operator, defining BGP routing policies, 264
applications, network evolution, 4
archiving logging messages, 140-141
area routers, 232
array cable
CRS-1 multishelf connections, 408-409, 418
LCC connections, 402
multishelf 2+1 systems, mapping in, 441-443
AS-path set, 261
ASBR (autonomous system boundary routers), OSPF, 212
ASIC (application-specific integrated circuits)
Fabricq ASIC, 55, 406
Ingressq ASIC, 55, 406
Qlink, 406
SEA, 406
ASR (Aggregation Service Router) 9000 systems, 14
asynchronous IPC, 32
attach-points, 258-259
auditing Cisco IOS XR installations/upgrades, 88-89
authentication
IS-IS configuration, 243-244
OSPFv2, 219, 221
RADIUS protocol, 172-173
router access, 161
SAM commands, 95
authorization, router access, 161
Auto-RP, configuring, 378-379
auto-rp candidate-rp command, 378
auto-rp mapping-agent command, 379
availability
carrier-grade NOS requirements, 5-6
high availability
architecture of, 50-53
CRS-1 multishelf, 405

B

BAA (bulkhead array adapters), OIM cards, 402
backbone routers, OSPF, 212
backpressure, 408
backups. ***See also*** disk mirroring
backup disks, 90-91
router configurations, 96
basic discovery (LSR), 302
BCDL (Bulk Content Downloader), 40-41
best path calculation, criteria, 248
BFD (Bidirectional Forwarding Detection) protocol
IS-IS configuration, 241-242

OSPFv2, 227-228
show bfd session command, 228
show process bfd detail location all command, 228
show running-config command, 228
BGP (Border Gateway Protocol), 293
address families, configuring, 251-252
best path calculation, 248
configuration groups, 252-256
configuring, 250-251
convergence
NHT, 288-290
reachability, 287
eBGP, CE-PE, 335-338
GR, 280-282
MP-iBGP, configuring, 320-324
policy accounting, 276-278
process placement, 45
routing policies
AS-path set, 261
Boolean operators, 264
community set, 261-262
example configuration, 266-272
hierarchical, 272-273
if statements, 263
inline sets, 264
parameterization, 274-276
prefix set, 259-261
redistribution attach-points, 258-259
RPL attributes, 264
RPL, 257
RTBH, configuring, 278-280
speakers, 248, 282-286
timers, 286-288
bgp graceful-restart command, 281
bgp router-id command, 251
blocking
processes, 25-26
RIP, 199-201
threads, 25-26
Boolean operators, defining BGP routing policies, 264
boot command, 438
boot process
DRP, determining success of, 389
ROMMON
booting .vm files, 73-75
BOOTLDR variable, 81
defining, 72
set command, 72
setting in TURBOBOOT, 72-73
routers, 59
standby RP, 82
TURBOBOOT
booting standby RP, 82
booting .vm files, 73-75
c12000 platform considerations, 81
package installations, 78-81
setting ROMMON variable, 72-73
verifying software installations, 76-78
.vm files, booting, 73-75
BOOT variable (ROMMON), 437
bootable files
composite bootable files, 63-65
downloading, 61-63
BOOTLDR variable (ROMMON), 81, 437
BOOT_DEV_SEQ_CONF variable (ROMMON), 90-91
BOOT_DEV_SEQ_OPER variable (ROMMON), 90-91
BPM (BGP Process Manager), 247

bRIB (BGP RIB), 249-250
BSR (Bootstrap Routers), 379

C

c12000 platform, TURBOBOOT considerations, 81
cable
array cable
CRS-1 multishelf connections, 408-409, 418
LCC connections, 402
mapping in multishelf 2+1 systems, 441-443
horizontal (multimodule) cabling, 409, 412
vertical (single-module) cabling, 409-412
candidate-bsr command, 379
carrier-grade NOS (network operating systems), 5-6
CE-PE (Customer Edge to Provider Edge), routing between
eBGP, 335-338
OSPF, 338-339
RIP, 339-340
static routing, 334
Cfgmgr LC process, 103
Cfgmgr RP process, 103
CFS (Configuration File System), 103
admin directory, 105
failed directory, 105
history directory, 105
lr directory, 105
primary persistent configuration, 105, 119-120
refpoints, 105-107
secondary persistent configuration, 107
checkpoint servers, 52
Cisco IOS XR
ASR 9000 systems, 14
boot process
booting standby RP, 82
booting .vm files, 73-75
package installations, 78-81
setting ROMMON variable, 72-73
verifying software installations, 76-78
control plane, 11
CRS-1, 13
data plane, 11
distribution models
load distribution model, 11
localization model, 10
EIGRP configuration, 204
NSF configuration, 207
NSF verification, 207
process status verification, 208-209
route policy configuration, 205-206
router ID configuration, 206
troubleshooting, 210-211
verifying, 210-211
forwarding, 12
high availability architecture, 50-53
image naming conventions, 60-61
installing
collaborating processes, 70
composite bootable files, 63-65
composite upgrade PIE (mini.pie), 65, 82-84
composite .vm files, 63-65
Configuration Manager, 70
downloading bootable files, 61-63
downloading PIE, 61-63
downloading SMU, 61-63

downloading .vm files, 61-63
image naming conventions, 60-61
install audits, 88-89
Install Director, 69-70
Install Helper (insthlper), 70
install rollback feature, 85-87
install subsystems, 70
instcmd process, 68
instdir process, 69-70
optional PIE, 65-67
package installations, 78-81
pkgfs process, 70
preparing for, 71-72
reloading routers, 63
removing inactive PIE, 87-88
router configuration backups, 96
Sysdb, 70
system overview, 67-70
testing PIE/SMU installations, 96
TURBOBOOT process, 72-82
verifying MD5 signatures, 95
verifying PIE/SMU config-registers, 96

IPC
ADR, 34
asynchronous IPC, 32
connection-oriented schemes, 33
GSP, 34, 36
inter-node IPC, 33
intra-node IPC, 33
LWM, 34
point-to-multipoint IPC, 34
point-to-point IPC, 34
Qnet, 35
rendezvous-oriented schemes IPC, 34
synchronous IPC, 31-32

IS-IS configuration, 234-235
authentication, 243-244
BFD configuration, 241-242
BFD verification, 241-242
interface state configuration, 238-239
IPFRR configuration, 242
IPFRR verification, 242
multitopology model, 237
NSF configuration, 239-240
NSF verification, 240
show isis database detail command, 233
single-topology command, 233
timer configuration, 239
troubleshooting, 245

IS-IS verification, 233-234
interface state verification, 238-239
multitopology model, 237
show isis database detail command, 235
show isis instance 1 command, 235-237
single topology model, 235-236

kernel
IPC, 23
modularity, 17
mutex, 24
POSIX compliance, 17
semaphore, 24
shared memory space, 23
synchronization services, 23-24
threads, 18-23

LPTS, 13
management plane, 11
microkernel architecture, 10

multicast routing
enabling, 377
IGMP configuration, 377
monitoring, 380-381
PIM configuration, 378
show run multicast-routing command, 380
static RP configuration, 378-379
troubleshooting, 380-382
OSPF configuration
BFD configuration, 227-228
BFD verification, 227-228
hierarchical CLI, 215-218
inheritance, 218-219
multiarea adjacency configuration, 226-227
multiarea adjacency verification, 226-227
NSF configuration, 221-223
NSR configuration, 224-226
NSR verification, 224-226
OSPFv2 authentication, 219-221
OSPFv2 configuration, 213
OSPFv2 verification, 213-214
OSPFv3 configuration, 229-230
OSPFv3 troubleshooting, 231
OSPFv3 verification, 230-231
standby RP status verification, 221-223
timer configuration, 229
overview of, 9-13
packet delivery, 13
partitioning, 12
performance, 13
PIE
composite upgrade PIE (mini.pie), 65, 82-84
downloading, 61-63
naming conventions, 60-61
optional PIE, 65-67
processes
cold processes, 52
hot processes, 52
placement of, 42-46
restarting, 51
SysDB processes, 47
warm processes, 52
RIP configuration, 196
blocking, 199-201
passive interface configuration, 199
restarting, 199-201
RPL configuration, 198
show process rip command, 199
show running-config command, 197-198
shutting down, 199-201
troubleshooting, 201-202
verifying, 201-202
routers, securing access, 161
scalability, 13
SDR, 12
security
router access, 161
software design, 159-160
SysDB
commit command, 47
configuring, 47-48
functions of, 46
processes, 47
show sysdb registration edm job location command, 50
show sysdb registrations notification command, 49-50
show sysdb registrations verification command, 49

system manager
functions of, 26-27
process attributes, 27, 30
process CLI, 29-31
process lifecycle, 28
processes, 28, 30
threads, displaying IS-IS thread names, 31
TURBOBOOT process
booting standby RP, 82
booting .vm files, 73-75
c12000 platform considerations, 81
package installations, 78-81
setting ROMMON variable, 72-73
verifying software installations, 76-78
upgrading
composite upgrade PIE (mini.pie), 82-84
disk space usage, 95-96
install audits, 88-89
install rollback feature, 85-87
reloading routers, 63
removing inactive PIE, 87-88
router configuration backups, 96
verifying PIE/SMU config-registers, 96
XR12000 systems, 14
cisco-support group, 162
Class D IP addresses, multicast routing, 357
clear command, 122
clear configuration inconsistency command, 120
clearing configuration sessions, 121-122
CLI (command-line interface)
Configuration Template feature, 128-129
OSPF, hierarchical CLI in, 215-218
processes, 29-31
cold processes, checkpoint servers, 52
collaborators, process restartability, 10
comment option (commit operation), 114
commit command, SysDB, 47
commit confirmed command, 115
commit model
commit operation, 112-113
available options, 114
failed configuration, 115-116
startup configuration failures, 116-117
two-stage, 110-112
commit operation, 112-113
available options, 114
confirmed option, 115
failed configuration, 115-116
startup configuration failures, 116-117
commit refpoints, 105-107
communication, IPC, 23
ADR, 34
asynchronous IPC, 32
connection-oriented schemes, 33
GSP, 34-36
inter-node IPC, 33
intra-node IPC, 33
LWM, 34
point-to-multipoint IPC, 34
point-to-point IPC, 34
Qnet, 35
rendezvous-oriented schemes, 34
synchronous IPC, 31-32
community set, 261-262
composite bootable files, Cisco IOS XR installations, 63-65

composite upgrade PIE (mini.pie), 65, 82-84
condvar (conditional variables), mutex priority inheritance, 24
config-register 0x102 command, 96
config-registers, verifying, 96
configuration groups (BGP), 252-256
configuration management
aborting sessions, 122
clearing sessions, 121-122
distributed model
CFS, 103-105
Configuration Manager, 101-103
control plane, 99
data plane, 99
RDSFS, 109-110
SysDB, 107-109
ending sessions, 122-123
OIR events, replacing SPA, 123-126
package activation/deactivation, 126-127
rollback, 102, 130-132
router startup, 129-130
Configuration Manager, 101
Cfgmgr LC process, 103
Cfgmgr RP process, 103
Cisco IOS XR installations, 70
configuration sessions
aborting, 122
clearing, 122
ending, 122-123
locking, 120
unlocking, 121
target configuration, exclusive sessions, 120-121
Configuration Navigation feature, 118
configuration planes, 100-101
configuration register, common settings table, 437
Configuration Template feature, 128-129
configuring
ACL, 179-180
Auto-RP, 378-379
BFD, OSPFv2, 227-228
BGP, 250
address families, 251-252
distributed speakers, 282-286
process placement, 45
routing policies, 266-272
RTBH, 278-280
CRS-1 multishelf
array cable connections, 418
LCC, 424-425
rack number assignments, 416
viewing configurations, 419-424
DRP, 388-392
EIGRP, 204
NSF configuration, 207
NSF verification, 207
process status verification, 208-209
route policy configuration, 205-206
router ID configuration, 206
IGMP, multicast routing, 377
IS-IS, 234-235
authentication, 243-244
BFD configuration, 241-242
interface state configuration, 238-239
IPFRR configuration, 242
mutlitopology model, 237
NSF configuration, 239-240

show isis database detail command, 233
single-topology command, 233
timer configuration, 239
LPTS, 191
MP-iBGP, 320-324
MPLS TE, 313-317
MPP, 177-178
multiarea adjacencies, OSPFv2, 226-227
NSF, 207, 221-223
NSR, OSPFv2, 224-226
OSPF
BFD configuration, 227-228
BFD verification, 227-228
hierarchical CLI, 215-218
inheritance, 218-219
multiarea adjacency configuration, 226-227
multiarea adjacency verification, 226-227
NSF configuration, 221-223
NSR configuration, 224-226
NSR verification, 224-226
OSPFv2 authentication, 219-221
OSPFv2 configuration, 213
OSPFv2 verification, 213-214
OSPFv3 configuration, 229-230
OSPFv3 verification, 230-231
standby RP status verification, 221-223
timer configuration, 229
PIM, 378
RIP, 196
passive interface configuration, 199
RPL configuration, 198
show running-config command, 197-198
routing policies (BGP)
community set, 261-262
prefix set, 259-260
RPL, 198
SDR, 389
SNMP, 137-138
SSH, 173-177
SSM, 379
static RP, 378-379
SysDB, 47-48
syslog, 139-140
TACACS+ servers, 171-172
VPWS, 341-345
VRF
PE configurations, 325-330
tables, 318-320
confirmed option (commit operation), 115
confreg command, 438
connection-oriented IPC schemes, 33
context switching, 8
control Ethernet, CRS-1 multishelf, 413-415
control plane, 11, 99
convergence
BGP, 286-290
carrier-grade NOS requirements, 5
cooperative multitasking systems, process scheduling, 7
core dumps
best practices, 154
generating, 148
core files, processes and, 30
CPU utilization, false positives from show system verify command output, 154
criteria for best path calculation, 248

CRS-1 (Carrier Routing System-1) multishelf, 13, 400
array cable connections, 408, 418
horizontal (multimodule) configurations, 412
recommended practices/ considerations, 409
vertical (single-module) configurations, 410-412
configuring
array cable connections, 418
LCC, 424-425
rack number assignments, 416
viewing configurations, 419-424
control Ethernet, 413-415
fabric planes, 401, 406
backpressure, 408
SEA links, 406-407, 429-434
troubleshooting, 426-428
FCC, 401
OIM cards, 402
OIM-LED cards, 402-403
power zones, 410-411
LCC, 401, 424-425
packet forwarding, 401
SFC, 404-405
CRS-DRP-B-CPU board (DRP), 388
CRS-DRP-PLIM board (DRP), 388
crypto key generate dsa command, 174
CSR routers, troubleshooting multicast routing, 381
current allocation location type, process placement, 43
cutover (switchover) process, 202

D

data plane
Cisco IOS XR, 11
configuration management, 99
data recovery
Golden Disk feature, 90-91
show system backup verify command, 90
system backup disk1 command, 90
data tables, BCDL, 40-41
databases
LSD, 295
SysDB
commit command, 47
configuring, 47-48
functions of, 46
processes, 47
show sysdb registration edm job location command, 50
show sysdb registrations notification command, 49-50
show sysdb registrations verification command, 49
de-aggregate label operation (MPLS), 296
deactivating packages, 126-127
debug commands, 163
debug pfilter-ea errors location command, 181
debug ssh server command, 174
debugging SSH, 174-177
default running configuration behavior, 119
DEFAULT_GATEWAY variable (ROMMON), 438
deleting physical interfaces, 117
DES (Data Encryption Standard), 135

describe command, 164
dir command, 104
discard notifications, backpressure and, 408
disk backups, 90-91
disk mirroring
enabling, 93
mirror location 0/rp0/CPU0 disk0:disk1 command, 93
monitoring, 94
partitions, 91-92
show mirror command, 94
disk space, Cisco IOS XR upgrades, 95-96
disk1: partition location 0/rp0/CPU0 force command, 93
distance vector protocols, 195
distributed configuration management
CFS, 103-107
Configuration Manager, 101-103
control plane, 99
data plane, 99
RDSFS, 109-110
SysDB, 107-109
Distributed Event Detector, 143
distributed speakers (BGP), 282-286
distribution models
load distribution model, 11
localization model, 10
DLL (dynamic link libraries), 9
dollar sign ($), RPL parameterization, 274
down flags (switch fabric), list of, 445-446
downstream unsolicited mode (LDP), 303
dr-priority command, PIM configuration, 378
DRP (distributed route processors)
booting, determining success of, 389
configuring, 388-390, 392
CRS-DRP-B-CPU board, 388
CRS-DRP-PLIM board, 388
DSDRSC, 387
pairing, 392
power zone distributions, 389
process placement, 397
SDR, 388
slot allocation, 389
DSA keys, generating, 174
DSC (Designated System Controllers), SDR, 388
DSDRSC (Designated Secure Domain Router System Controllers), 43, 386
DUAL (Diffusing Update Algorithm), 204
dumpcore command, 148
dynamic state recovery, 52

E

eBGP, CE-PE, 335-338
editing BGP routing policies, 261
EEM (Embedded Event Manager), 135, 141
Distributed Event Detector, 143
None Event Detector, 142
policies
registering, 142-144
user-defined, 144-146
reliability metrics, 146-147
Syslog Event Detector, 142
System Manager Event Detector, 142
Timer Services Event Detector, 142
Watchdog System Event Detector, 143

egress paths (CSR routers), troubleshooting multicast routing, 381

egress PSE, forwarding paths, 55

EIGRP (Enhanced Interior Gateway Routing Protocol)

configuring, 204

NSF configuration, 207

NSF verification, 207

process status verification, 208-209

route policy configuration, 205-206

router ID configuration, 206

DUAL, 204

fundamentals of, 203

Neighbor Discovery/Recovery, 203

protocol-dependent modules, 204

RTP, 203

troubleshooting, 210-211

verifying, 210-211

end command, 122-123

ending configuration sessions, 122-123

error messages, troubleshooting running configurations, 119

ES (end systems), 232

Ethernet, CRS-1 multishelf, 413-415

event detectors (EEM), 142-143

event manager policy command, 142

example RPL policy configuration, 266-272

exclusive target configuration sessions, 120-121

exec subblock, instcmd process, 68

executable paths, 30

exit command, 122-123

extended discovery (LSR), 303

extended keywords, ACL, 179

external AAA, router access security, 169-173

F

fabric plane

CRS-1 multishelf, 401

backpressure, 408

SEA links, 406-407, 429-434

troubleshooting in, 426-428

multicast routing, troubleshooting, 381

no controllers fabric rack 1 install-mode command, 425

show controller fabric plane [n] command, 425

UCE, troubleshooting, 381

Fabricq ASIC, 55, 406

failed configuration, 115-116

failed directory (CFS), 105

failures

detecting, carrier-grade NOS, 6

during startup configuration, 116-117

recovery, carrier-grade NOS, 5

false positives, from show system verify command output, 154

FCC (fabric card chassis)

CRS-1 multishelf, 401-403

power zones, 410-411

rack number assignments, 416

FEC (fowarding equivalence class), MPLS, 293

FGID (Fabric Group Identifiers), multicast routing, 361

FIFO (first in first out) scheduling, 21

filtering ACL, 178-181

firewalls, LPTS, 13, 185

flexibility of services, carrier-grade NOS requirements, 6

follow process command, 148

Forward flags, sparse mode forwarding, 370

forwarding
- Cisco IOS XR, 12
- Reverse Path Forwarding, 359

forwarding paths, 54-55

forwarding plane (routers), security
- ACL filtering, 178-181
- defining, 159
- LPTS, 183-191
- uRPF, 181-182

FRR (Fast Re-Routing), MPLS TE, 312

G - H

generating core dumps, 148

Get messages (SNMP), 136

GID number allocation (GSP), 36

Golden Disk feature, disk backups via, 90-91

GR (graceful restart), 280, 282

GSP (Group Service Protocol), 34
- BCDL, 40-41
- GID number allocation, 36
- show gsp groups location command, 38-39
- show gsp stats client location command, 37

HA (high availability), CRS-1 multishelf, 405

hardware, redundancy, 5

hello-interval command, PIM configuration, 378

hello-password command, IS-IS authentication, 243

hfr-mcast-p.pie (mcast pie), 66

hierarchical BGP routing policies, 272-273

hierarchical CLI, OSPF, 215-218

high availability
- BGP GR, 280-282
- WDSYSMON, 149-150

high availability architecture, 50-53

history directory (CFS), 105

HMAC (Hashed Message Authentication Code), 135

hop-counts, RIP, 195

horizontal (multimodule) cabling, CRS-1 multishelf connections, 409, 412

hot processes, checkpoint servers, 52

hot standbys, OSPF, 224

hw-module location command, 156

hw-module reset auto disable location command, 156

hw-module shutdown location command, 156

I

ICMP unreachables, ACL, 179

if-then-else statements, defining BGP routing policies, 263

IGMP (Internet Group Management Protocol), multicast routing, 357-358, 377

IGP (Interior Gateway Protocols)
- EIGRP
  - *configuring, 204-209*
  - *DUAL, 204*
  - *fundamentals of, 203*
  - *Neighbor Discovery/Recovery, 203*
  - *protocol-dependent modules, 204*
  - *RTP, 203*
  - *troubleshooting, 210-211*
  - *verifying, 210-211*

IS-IS
configuring, 233-244
IS hellos, 233
Level 1 routing, 232
Level 2 routing, 232
NET, 232
NSAP, 232
SDF, 232
SIF, 232
troubleshooting, 245
verifying, 233-242
OSPF
ABR, 212
ASBR, 212
backbone routers, 212
configuring, 213-231
hot standbys, 224
internal routers, 212
LSA, 212
LSDB, 211
NSSA, 212
OSPFv2, 212
OSPFv3, 212
process restart ospf command, 222
show ospf command, 229
show ospf standby command, 224
show ospf standby database command, 223
show running-config router ospf command, 224
stub areas, 212
throttle command, 229
timers lsa min-interval command, 229
troubleshooting, 231
warm standbys, 221-222
RIP
blocking, 199-201
configuring, 196-199
hop-counts, 195
passive configuration command, 196
restarting, 199-201
RIPv1, 196
RIPv2, 196
route update intervals, 195
show process rip command, 199
shutting down, 199-201
troubleshooting, 201-202
verifying, 201-202
image naming conventions, 60-61
incoming interfaces, multicast routing, 359
independent label distribution control mode (LDP), 303
ingress paths (CSR routers), troubleshooting multicast routing, 381
ingress PSE, forwarding paths, 55
Ingressq ASIC, 55, 406
inheritance
OSPF, 218-219
task groups, 167-168
user groups, 167-168
inline sets, 264
install commit command, 79, 84
install deactivate command, 85, 88
Install Director, 69-70
Install Helper (insthlper), Cisco IOS XR installations, 70
Install Manager
Cisco IOS XR installations, system overview, 67-70
install deactivate command, 88
install remove command, 88

PIE, validating, 95
SMU, validating, 95
install remove command, 88
install remove inactive command, 87
install rollback feature, 85-87
install-mode (LCC), 424
installing
Cisco IOS XR
collaborating processes, 70
composite bootable files, 63-65
composite upgrade PIE (mini.pie), 65, 82-84
composite .vm files, 63-65
Configuration Manager, 70
downloading bootable files, 61-63
downloading PIE, 61-63
downloading SMU, 61-63
downloading .vm files, 61-63
image naming conventions, 60-61
install audits, 88-89
Install Director, 69-70
Install Helper (insthlper), 70
install rollback feature, 85-87
install subsystems, 70
instcmd process, 68
instdir process, 69-70
optional PIE, 65-67
package installations, 78-81
pkgfs process, 70
preparing for, 71-72
reloading routers, 63
removing inactive PIE, 87-88
router configuration backups, 96
Sysdb, 70
system overview, 67-70
testing PIE/SMU installations, 96
TURBOBOOT process, 72-82
verifying MD5 signatures, 95
verifying PIE/SMU config-registers, 96
install commit command, 79, 84
install deactivate command, 88
install remove command, 88
install remove inactive command, 87
packages, 78-81
show install active summary command, 87
show install detail command, 76-78
show install inactive command, 87
show install log command, 87
show install log from command, 84-85
show install request command, 87
show install summary command, 76
SMU, 67
software, verifying installations, 76-78
instances (process), 30
instcmd process, 68
instdir process, 69-70
inter-node IPC (interprocess communication), 33
interface forward referencing, 99
interface preconfiguration, 127-128
interface states (IS-IS), configuring, 238-239
interfaces (physical), deleting, 117
internal routers, OSPF, 212
interrupt handling, 8
interrupt masking, 8
intra-node IPC (interprocess communication), 33
IP addresses, Class D IP addresses, 357
IPC (interprocess communication), 9
ADR, 34
asynchronous IPC, 32
connection-oriented schemes, 33

GSP, 34
BCDL, 40-41
GID number allocation, 36
show gsp groups location command, 38-39
show gsp stats client location command, 37
inter-node IPC, 33
intra-node IPC, 33
kernel synchronization, 23
LWM, 34
point-to-multipoint IPC, 34
point-to-point IPC, 34
Qnet, 35
rendezvous-oriented schemes, 34
synchronous IPC, 31-32
IPFRR (IP Fast Reroute), 242
ipfrr lfa level 1|2 command, 242
IPv4 multicast routing, 356
Class D IP addresses, 357
enabling, 377
FGID, 361
fundamentals of, 357
IGMP, 357-358, 377
incoming interfaces, 359
MBGP, 361
MFIB, 361, 365-366, 369, 382
monitoring, 380-381
MPA, 360
MRIB, 361, 365-367, 370-372
muRIB, 361
PIM, 357
configuring, 378
show pim rpf command, 382
SM protocol, 359, 362-374
SSM, 374-379
Reverse Path Forwarding, 359
RPF neighbors, 359
shared trees, 359
show run multicast-routing command, 380
SPT, 359
static RP configuration, 378-379
troubleshooting, 380-382
IP_ADDRESS variable (ROMMON), 438
IP_SUBNET_MASK variable (ROMMON), 438
IS (intermediate systems), routers as, 232
IS hellos, 233
IS-IS (Intermediate System to Intermediate System)
configuring, 233-235
authentication, 243-244
BFD configuration, 241-242
BFD verification, 241-242
interface state configuration, 238-239
IPFRR configuration, 242
IPFRR verification, 242
multitopology model, 237
NSF configuration, 239-240
NSF verification, 240
show isis database detail command, 233
single-topology command, 233
timer configuration, 239
IS hellos, 233
Level 1 routing, 232
Level 2 routing, 232
NET, 232
NSAP, 232
SDF, 232
SIF, 232
thread names, displaying, 31

troubleshooting, 245
verifying, 233-234
interface state verification, 238-239
multitopology model, 237
show isis database detail command, 235
show isis instance 1 command, 235-237
single topology model, 235-236
ispf [level { 1 | 2}] command, 240
item tokens, 28

J - K - L

JID (job ids), 28, 30

KAT (Keep Alive Timers), sparse mode forwarding, 369-370
kernel
defining, 8
kernel-based OS (operating systems), 8
modularity, 17
POSIX compliance, 17
synchronization, 23-24
threads, 18-23
keywords, ACL, 179
ksh command, 92

L2VPN (Layer 2 Virtual Private Networks), 340
pseudo wire redundancy, 346-347
show l2vpn bridge-domain brief command, 350-353
show l2vpn forwarding summary location command, 350
show l2vpn xconnect command, 343
show l2vpn xconnect neighbor command, 346
VPLS, 347-353
VPWS, 340
configuring, 341-345
local switching, 344
L3VPN (Layer 3 Virtual Private Networks)
MP-1BGP, configuring, 320-324
VRF tables, 318-320
last started date and time timestamp (processes), 30
LCC (line card chassis)
array cable connections, 402
CRS-1 multishelf, 401, 424-425
install-mode, 424
rack number assignment, 416
LDP (Label Distribution Protocol), 293, 309
basic configuration, 305-306
downstream unsolicited mode, 303
independent label distribution control mode, 303
label binding, 303-304
label control, 306-308
LDP-IGP synchronization, 310-312
liberal label retention mode, 303
LSR discovery, 302-303
parameters of, 306
session protection, 310-311
show mpls ldp discovery command, 343
Level 1 routing (IS-IS), 232
Level 2 routing (IS-IS), 232
level tokens, 27
Libc (C standard libraries), 9
liberal label retention mode (LDP), 303
line numbering, ACL, 179

link state protocol, LSA, 212
link state protocols, 195, 211
load balancing, MPLS, 299-302
load distribution models, 11
loadpaths, 70
local plane, 101
local switching (VPWS), 344
Local SysDB Server, 108
localization distribution models, 10
locking configuration sessions, 120
log messages (ACL), 179
log-traps command, troubleshooting multicast routing, 380
logging, syslog
- best practices, 154
- destination, configuring, 139-140
- messages, 138
  - *archiving, 140-141*
  - *severity levels, 139*

logging buffer, configuring, 140
logging command, 140
logical routers (root-lr), 162
logins, named SDR, 395-397
LPTS (Local Packet Transport Service), 13, 183
- BGP entries in, 186-190
- configuring, 191
- firewalls, 185
- overview of, 186

lr directory (CFS), 105
LSA (link state advertisement), 212
LSD (Label Switch Databases), 295
LSDB (link state databases), 211
lsp-gen-interval [level { 1 | 2}] command, 240
lsp-interval milliseconds [level { 1 | 2}] command, 240
lsp-password command, IS-IS authentication, 243
LSR (Label Switch Routers)
- label binding, 304
- LDP discovery, 302-303
- penultimate hop popping, 294-296
- TL processing, 299
- ultimate-hop popping, 294

LWM (Light Weight Messaging), 34

M

mainline releases, naming conventions, 60-61
maintenance releases, naming conventions, 60-61
managed devices (SNMP), traps, 136
managed objects, 136
management plane, 11, 177-178
mandatory processes, 31
mandatory tokens, 28
Max. core files, processes and, 30
max spawns per minute (processes), 30
MBGP (Multicast BGP), 361
mcast pie (hfr-mcast-p.pie), 66
MD5 signatures, verifying, 95
memory
- core files, process attributes, 30
- memory protection, 8
- monitoring, WDSYSMON, 149-150
- network evolution, 4
- oom-handling command, troubleshooting multicast routing, 380
- shared memory, 8, 23

memory comparison tool, 150-151
messages
- ADR, 34

GSP, 34
BCDL, 40-41
GID number allocation, 36
show gsp groups location command, 38-39
show gsp stats client location command, 37
LWM, 34
Qnet, 35
syslog, 138
archiving, 140-141
destination, configuring, 139-140
MFIB (Multicast Forwarding Information Base)
MFIB command, troubleshooting RPF failures, 382
multicast routing, 361, 365-366, 369, 382
MFWD (Multicast Forwarding), multicast routing, 361
MIB (Management Information Base), 135-136
microkernel
Cisco IOS XR overview, 10
modularity, 17
POSIX compliance, 17
synchronization, 23-24
threads, 18-23
mini.pie (composite upgrade PIE), 65, 82-84
mirror location 0/rp0/CPU0 disk0:disk1 command, 93
mirroring disks. *See also* backups
enabling, 93
mirror location 0/rp0/CPU0 disk0:disk1 command, 93
monitoring, 94
partitions, 91-92
show mirror command, 94
modularity (kernel), 17
monitor controller fabric plane all command, 155
monitor controller sonet command, 155
monitor interface command, 155
monitor processes location command, 148
monitor threads location command, 148
monitoring
best practices, 154-156
memory, 149-151
multicast routing, 380-381
processes
related commands, 147
WDSYSMON, 149-150
monolithic operating systems, 8
MP-iBGP (multi-protocol internal iBGP), configuring, 320-324
MPA (Multicast Policy Areas), multicast routing, 360
MPLS (Multi-Protocol Label Switching)
architecture of, 294-296
BGP, 293
control protocols, corresponding FEC type table, 293
defining, 292
FEC, corresponding MPLS control protocol table, 293
LDP, 293, 309
basic configuration, 305-306
downstream unsolicited mode, 303
independent label distribution control mode, 303
label binding, 303-304
label control, 306-308
LDP-IGP synchronization, 310-312
liberal label retention mode, 303
LSR discovery, 302

mpls ldp discovery command, 343
parameters of, 306
session protection, 310-311
load balancing, 299-302
LSD, 295
LSR
label binding, 304
LDP discovery, 302
penultimate hop popping, 294-296
TTL processing, 299
ultimate-hop popping, 294
MPLS TE, 312-317
MSVP, 293
packet forwarding
de-aggregate label operation, 296
load balancing, 299-302
pop label operation, 296
push label operation, 296
show mpls forwarding command, 296-298
show mpls forwarding prefix command, 305
show mpls label table command, 298
swap and push label operation, 296
swap label operation, 295
unlabeled label operation, 296
VPN
common show commands table, 330
connectivity options, 324-325
RD values in VPN routes, 330-333
VRF configuration, 325-330
MPP (Management Plane Protection), 177-178
MRIB (multicast routing information base), 361, 365-367, 370-372
MSC (Modular Services Cards), forwarding paths, 54-55
multi-area-interface command, 226
multiarea adjacencies, OSPFv2 configuration, 226-227
multicasting routing, 356
Class D IP addresses, 357
enabling, 377
FGID, 361
fundamentals of, 357
IGMP, 357-358, 377
incoming interfaces, 359
MBGP, 361
MFIB, 361, 365-366, 369, 382
monitoring, 380-381
MPA, 360
MRIB, 361, 365-367, 370-372
muRIB, 361
PIM, 357
configuring, 378
show pim rpf command, 382
SM protocol, 359, 362-374
SSM, 374-379
Reverse Path Forwarding, 359
RPF neighbors, 359
shared trees, 359
show run multicast-routing command, 380
SPT, 359
static RP configuration, 378-379
troubleshooting, 380-382
multimodule (horizontal) cabling, CRS-1 multishelf connections, 409, 412
multishelf 2+1 systems, array cable mapping, 441-443
multitasking systems, 7
multithreaded operating systems, 8

muRIB (multicast unicast routing information base), 361
mutex (mutual exclusion lock), 24

N

name tokens, 27
named access lists (ACL), 179
named SDR (Secure Domain Routers)
creating, 392
logins, 395-397
resources, assigning, 393-395
naming conventions, Cisco IOS XR, 60-61
Neighbor Discovery/Recovery (EIGRP), 203
neighbor-group BGP configuration group, 252-256
NET (Network Entity Title), 232
netadmin group, 162
network operators, 3-4
networks
evolution of
applications, 4
memory capacities, 4
network operators, 3-4
network services, 4
processors, 4
protocols, 3-4
routers, 3
transmission capacities, 4
user size, 4
management, SNMP, 135
configuring, 137
Get messages, 136
managed devices, 135
MIB, 135
NMS, 135
Set messages, 136
supported versions, 135
traps, 136-137
VRF instances, configuring in, 138
NHT (Next Hop Tracking), BGP reachability notifications, 288-290
NMS (Network Management Station), 135
no controllers fabric rack 1 install-mode command, 425
nodes, OIR, 123-126
non-owner SDR (Secure Domain Routers), 385-386
None Event Detector, 142
NOS (network operating systems), carrier-grade NOS, 5-6
NOT Boolean operator, BGP routing policies, 264
notifications, EEM, 141
NS (Negate Signal), sparse mode forwarding, 370
NSAP (Network Service Access Point), 232
NSF (nonstop forwarding)
configuring, 207
IS-IS configuration, 239-240
OSPFv2 configuration, verifying, 221-223
verifying, 207
NSR (nonstop routing), OSPFv2 configuration, 224-226
NSSA (not-so-stubby areas), OSPF, 212
NTP (Network Time Protocol), best practices, 154

O

OIM (optical interface module) cards, CRS-1 multishelf, 402

OIM-LED (optical interface module light emitting diode) cards
CRS-1 multishelf, 402-403
LED states, 403
OIR (online insertion and removal), replacing SPA, 123-126
one fabric card chassis, 404
one line card chassis, 404
oom-handling (out of memory handling) command, troubleshooting multicast routing, 380
operations best practices, 154-156
operator groups, 162
operators (network), network evolution, 3-4
optical array cable, CRS-1 multishelf connections, 408-409, 418
optional PIE (Package Installation Envelopes), 65-67
OR Boolean operator, defining BGP routing policies, 264
OS (operating systems)
DLL, 9
interrupt handling, 8
IPC, 9
kernel-based OS, 8
Libc, 9
memory management, 8
monolithic operating systems, 8
multithreaded operating systems, 8
POSIX, 9
process scheduling, 7
synchronization, 9
OSPF (Open Shortest Path First)
ABR, 212
ASBR, 212
backbone routers, 212
CE-PE, 338-339
configuring
BFD configuration, 227-228
BFD verification, 227-228
hierarchical CLI, 215-218
inheritance, 218-219
multiarea adjacency configuration, 226-227
multiarea adjacency verification, 226-227
NSF configuration, 221-223
NSR configuration, 224-226
NSR verification, 224-226
OSPFv2 authentication, 219-221
OSPFv2 configuration, 213
OSPFv2 verification, 213-214
OSPFv3 configuration, 229-230
OSPFv3 verification, 230-231
standby RP status verification, 221-223
timer configuration, 229
hot standbys, 224
internal routers, 212
LSA, 212
LSDB, 211
NSSA, 212
OSPFv2, 212
OSPFv3, 212
process restart ospf command, 222
show ospf command, 229
show ospf standby command, 224
show ospf standby database command, 223
show running-config router ospf command, 224
stub areas, 212
throttle command, 229
timers lsa min-interval command, 229

troubleshooting, 231
warm standbys, 221-222
owner SDR (Secure Domain Routers), 385-386

P

packages
activation/deactivation, 126-127
installing, 78-81
packet delivery, LPTS, 13
packet forwarding
CRS-1 multishelf, 401
forwarding paths, 54-55
forwarding plane, 159
MPLS
de-aggregate label operation, 296
load balancing, 299-302
pop label operation, 296
push label operation, 296
show mpls forwarding command, 296-298
show mpls forwarding prefix command, 305
show mpls label table command, 298
swap and push label operation, 296
swap label operation, 295
unlabeled label operation, 296
paired allocation location type, process placement, 43
pairing DRP (distributed route processors), 392
parameterization, 274-276
parser subblock, instcmd process, 68
partitions, 12
disk mirroring
creating partitions for, 92
ratios table, 91
Disk1: partition location 0/rp0/CPU0 force command, 93
ksh command, 92
passive command, IS-IS interface state configuration, 238
passive configuration command, 196
passive RIP interfaces, configuring, 199
patches (software), carrier-grade NOS, 6
path tokens, 27
PE (provider edge)
CE-PE
eBGP, 335-338
OSPF, 338-339
RIP, 339-340
static routing, 334
pseudo wire redundancy, 346-347
routers
MP-iBGP, 320-324
VRF configuration, 325-330
penultimate hop popping, 294-296
performance, Cisco IOS XR, 13
physical interfaces, deleting, 117
PID (process IDs), 28-30
PIE (Package Installation Envelopes)
composite upgrade PIE (mini.pie), 65, 82-84
config-registers, verifying, 96
downloading, 61-63
inactive PIE, removing from Cisco IOS XR upgrades, 87-88
install deactivate command, 85
mcast pie (hfr-mcast-p.pie), 66
MD5 signatures, verifying, 95
naming conventions, 60-61
optional PIE, 65-67
testing installations, 96
validating, 95

PIM (Protocol Independent Multicast)
multicast routing, 357, 359
configuring, 378
SM protocol, 359, 362-374
SSM, 374-379
show mrib route command, 365-367
show pim interface command, 365
show pim rpf command, 367, 382
show pim topology command, 366-369
SM protocol, 359, 362-374
ping control-eth location command, 35
pkgfs process, Cisco IOS XR installations, 70
placement reoptimize command, 46
PLIM (Physical Layer Interface Modules), forwarding paths, 54-55
point-to-multipoint IPC (interprocess communication), 34
point-to-point IPC (interprocess communication), 34
policies (EEM)
registering, 142-144
user-defined, 144-146
policy accounting (BGP), 276-278
policy repository, 258
pop label operation (MPLS), 296
POSIX (Portable Operating System Interface), 9, 17
power zones
DRP, 389
FCC, 410-411
preconfiguration, 127-128
preemptive multitasking systems, process scheduling, 7
prefix sets, 259-261
primary allocation location type, process placement, 43
primary persistent configuration, 102, 105
router configuration, restoring, 129-130
running configurations, troubleshooting, 119-120
priority inheritance
condvar, 24
mutex, 24
threads, 20
priority inversion, 20
process restart ospf command, 222
processes
attributes of, 27, 30
blocked processes, 25-26
BPM, 247
CLI, 29-31
cold processes, checkpoint servers, 52
common process states, 24-25
context switching, 8
core files, 30
defining, 7
executable paths, 30
hot processes, checkpoint servers, 52
instances, 30
IPC, 23
ADR, 34
asynchronous IPC, 32
connection-oriented schemes, 33
GSP, 34-36
inter-node IPC, 33
intra-node IPC, 33
LWM, 34
point-to-multipoint IPC, 34
point-to-point IPC, 34
Qnet, 35
rendezvous-oriented schemes, 34
synchronous IPC, 31-32

item tokens, 28
JID, 28-30
last started date and time timestamp, 30
level tokens, 27
lifecycle of, 28
mandatory processes, 31
mandatory tokens, 28
max spawns per minute, 30
memory comparison tool, 150-151
monitoring, 147-150
name tokens, 27
path tokens, 27
PID, 28, 30
placement of, 397
affinity, 42-43
BGP processes, 45
placement reoptimize command, 46
show placement policy program [bgp] instance command, 45
show placement program all command, 43, 45
respawn counts, 30
restarting, 6, 10, 51
scheduling, 7
security, 160
show process boot location command, 27
show process location command, 29-30
show process pidin command, 22-23
show process pidin location command, 24
show process threadname command, 31
show processes blocked location command, 25-26
show processes threadname 120 command, 18
start on config, 30
state of, 30
SysDB (System Database) processes, 47
TID, 30
warm processes, checkpoint servers, 52
processors, network evolution, 4
protocol-dependent modules, EIGRP and, 204
protocols, network evolution, 3-4
pseudo wire redundancy, 346-347
push label operation (MPLS), 296

Q - R

Qlink ASIC, 406
Qnet, 35

RA (Really Alive), sparse mode forwarding, 370
RADIUS protocol
authentication via, 172-173
router access security, 169
rate-per-route command, troubleshooting multicast routing, 380
RDSFS (Replicated Data Service File System), 109-110
reachability, BGP NHT, 288-290
recovery
data recovery, 90-91
failure recovery, carrier-grade NOS, 5
redistribution attach-points, 258-259
redundancy
hardware, carrier-grade NOS, 5
pseudo wire redundancy, 346-347
refpoints, 105
absolute, 107
commit, 107
rollbacks, 130

registering EEM policies, 142-144
reliability metrics for EEM, 146-147
reload location all command, 96
remarks (ACL), 179
rendezvous-oriented IPC schemes, 34
replacing SPA, 123-126
resequencing ACL, 179
reset command, 438
respawn counts (processes), 30
restartability (processes)
carrier-grade NOS, 6
Cisco IOS XR, 10
collaborators, 10
restarting
processes, 51
RIP, 199-201
restoring router configuration, 129-130
Reverse Path Forwarding, 359
rewrites (LSD), 295
RIB (Routing Information Base), BGP next hops
NHT, 288-290
reachability, 287
RIP (Routing Information Protocol)
blocking, 199-201
CE-PE, 339-340
configuring, 196
passive interface configuration, 199
RPL configuration, 198
show running-config command, 197-198
hop-counts, 195
passive configuration command, 196
restarting, 199-201
RIPv1, 196
RIPv2, 196
route update intervals, 195
show process rip command, 199
shutting down, 199-201
troubleshooting, 201-202
verifying, 201-202
rollback, 102, 130-132
ROMMON (ROM Monitor)
boot command, 438
BOOT variable, 437
BOOT_DEV_SEQ_CONF variable, 90-91
BOOT_DEV_SEQ_OPER variable, 90-91
BOOTLDR variable, 81, 437
confreg command, 438
DEFAULT_GATEWAY variable, 438
defining, 72
IP_ADDRESS variable, 438
IP_SUBNET_MASK variable, 438
reset command, 438
set command, 72, 438
sync command, 438
TFTP_FILE variable, 438
TURBOBOOT variable, 72-73, 438
unset command, 438
root-lr (logical routers), 162
root-system group, 162
root-system users, 161
round-robin scheduling, 21-23
route leaking, 250
route update intervals, 195
router bgp command, 250
router pim address-family ipv6 command, PIM configuration, 378
routers
ABR, OSPF, 212

access security
- *AAA accounting, 161*
- *AAA authentication, 161*
- *AAA authorization, 161*
- *admin plane, 161*
- *external AAA, 169-173*
- *MPP, 177-178*
- *RADIUS protocol, 169*
- *SDR plane, 161-162*
- *SSH, 173-177*
- *TACACS+ protocol, 169-172*
- *task groups, 162-168*
- *telnet ipv4 server max-servers command, 161*
- *user groups, 162-168*

area routers, 232
ASBR, OSPF, 212
backbone routers, OSPF, 212
booting, 59
BSR, 379
Cisco IOS XR boot process
- *booting standby RP, 82*
- *booting .vm files, 73-75*
- *package installations, 78-81*
- *setting ROMMON variable, 72-73*
- *verifying software installations, 76-78*

configuration backups, 96
CSR routers, troubleshooting multicast routing, 381
DSDRSC, 386
forwarding pane
- *ACL filtering, 178-181*
- *LPTS, 183-191*
- *uRPF, 181-182*

internal routers, OSPF, 212
IS, 232
LSR
- *label binding, 304*
- *LDP discovery, 302*
- *penultimate hop popping, 294-296*
- *TTL processing, 299*
- *ultimate-hop popping, 294*

management plane, MPP, 177-178
network evolution, 3
PE routers
- *MP-iBGP, 320-324*
- *VRF configuration, 325-330*

PIM SM protocol, 359, 362-374
reloading, 63
root-lr (logical routers), 162
SDR, 384
- *Cisco IOS XR, 12*
- *configuring, 389*
- *creating, 388*
- *dedicated resources, 387*
- *DRP configuration, 388-392*
- *DRP pairings, 392*
- *DSDRSC, 386*
- *named SDR creation, 392-395*
- *named SDR logins, 395-397*
- *non-owner SDR, 385-386*
- *owner SDR, 385-386*
- *privileges, 387*
- *shared resources, 387*
- *show sdr summary command, 385, 394*

security, 6
SMU installations, 67
stations, 232

routing (multicast), 356

Class D IP addresses, 357
enabling, 377

- FGID, 361
- fundamentals of, 357
- IGMP, 357-358, 377
- incoming interfaces, 359
- MBGP, 361
- MFIB, 361, 365-366, 369, 382
- monitoring, 380-381
- MPA, 360
- MRIB, 361
- muRIB, 361
- PIM, 357-359, 362-379
- Reverse Path Forwarding, 359
- RPF neighbors, 359
- shared trees, 359
- show run multicast-routing command, 380
- SPT, 359
- static RP configuration, 378-379
- troubleshooting, 380-382

routing policies
- BGP
  - *AS-path set, 261*
  - *Boolean operators, 264*
  - *community set, 261-262*
  - *example configuration, 266-272*
  - *hierarchical policies, 272-273*
  - *if statements, 263*
  - *inline sets, 264*
  - *policy accounting, 276, 278*
  - *prefix sets, 259-261*
  - *RPL attributes, 264*
  - *RPL parameterization, 274-276*
- policy repository, 258
- redistribution attach-points, 258-259

routing protocols
- distance vector protocols, 195
- interface forward referencing, 99
- link state protocols, 195
  - *LSA, 212*
  - *LSDB, 211*

RP (Rendezvous Points)
- failovers, reasons for, 53
- processes, placement of, 42-46
- redundancy, best practices, 154
- shared trees, 359
- standby RP
  - *booting, 82*
  - *resetting, 91*
  - *troubleshooting, 91*
  - *verifying status, 221-223*
- static RP
  - *Auto-RP configuration, 378-379*
  - *BSR configuration, 379*
  - *multicast routing configurations, 378-379*
- switchover (cutover) process, 202

rp-address command, static RP configuration, 378

RPF (Reverse Path Forwarding)
- neighbors, multicast routing, 359
- troubleshooting, MFIB command, 382

RPL (Route Policy Language), 257
- attributes, 264
- configuring, 198
- parameterization, 274-276
- policy accounting, 276-278
- routing policies, 262
  - *Boolean operators, 264*
  - *example configuration, 266-272*
  - *hierarchical, 272-273*
  - *if-then-else statements, 263*
  - *inline sets, 264*

RSVP (Resource Reservation Protocol), 293

RTBH (remotely triggered black hole), configuring, 278-280
RTP (Reliable Transport Protocol), 203
running configuration. *See also* startup configuration
commit operation, 112-113
available options, 114
confirmed option, 115
failed configuration, 115-116
default behavior, 119
viewing with Configuration Navigation feature, 118

S

S2 cards. *See* SFC (switch fabric cards)
SAM (Software Authentication Manager) command, 95
SC (shelf controller) function, multishelf control Ethernet, 413
scalability
carrier-grade NOS requirements, 5
Cisco IOS XR, 13
scheduling
processes, 7
threads, 19
FIFO scheduling, 21
round-robin scheduling, 21-23
sporadic scheduling, 21
scripts, EEM, 143-144
SDF (subnetwork dependent functions), 232
SDR (Secure Domain Routers)
Cisco IOS XR, 12
configuration planes, 100-101
configuring, 389
creating, 388
dedicated resources, 387
DRP, 388-392
DSDRSC, 386
named SDR
assigning resources to, 393-395
creating, 392
logins, 395-397
non-owner SDR, 385-386
owner SDR, 385-386
privileges, 387
router access security, 161-162
shared resources, 387
show sdr summary command, 385, 394
SEA (switch fabric elements), CRS-1 multishelf
Fabricq ASIC, 406
Ingressq ASIC, 406
Qlink ASIC, 406
SEA ASIC, 406
troubleshooting, 429-434
SEA ASIC, 406
secondary persistent configuration, 102, 107
security
ACL filtering, 178-181
carrier-grade NOS requirements, 6
processes, 160
router access, 6
AAA accounting, 161
AAA authentication, 161
AAA authorization, 161
admin plane, 161
external AAA, 169-173
MPP, 177-178
RADIUS protocol, 169
SDR plane, 161-162
SSH, 173-177
TACACS+ protocol, 169-172

task groups, 162-168
telnet ipv4 server max-servers command, 161
user groups, 162-168
software, 159-160
semaphore, 24
send brk command, 91
servers
processes, SysDB, 108
TACACS+ server configuration, 171-172
serviceadmin group, 162
services
flexibility of, carrier-grade NOS requirements, 6
network evolution, 4
session-group BGP configuration group, 252-256
set command, 72, 438
Set messages (SNMP), 136
set rip-metric option, RIP configuration, 198
severity levels of syslog messages, 139
SFC (switch fabric cards), CRS-1 multishelf, 404-405
shared memory, 8, 23
shared plane, 100
shared trees, multicast routing, 359
Shared/Global SysDB Server, 108
show commands
MPLS VPN, common show commands table, 330
show l2vpn bridge-domain brief command, 350-353
show l2vpn forwarding summary location command, 350
show l2vpn xconnect command, 343, 346
show aaa task supported command, 162
show access-lists afi-all command, 181
show access-lists hardware location command, 181
show access-lists maximum command, 181
show access-lists usage pfilter location command, 181
show bfd session command, BFD configuration, 228
show bgp process command, 286-288
show bgp vpnv4 unicast summary command, 322
show cef resource detail location command, 155
show config merge command, 111
show config session command, 121
show config sessions command, 120
show configuration command, 111
show configuration commit changes command, 113
show configuration failed command, 115
show configuration failed startup command, 116
show configuration history command, 105, 132
show configuration removed command, 126
show context command, 155
show context location all command, 148
show controller fabric link port [s2rx] all statistics command, 433
show controller fabric plane [n] command, 425
show controllers fabric bundle all detail command, 431
show controllers fabric bundle port all command, 429
show controllers fabric link port ? command, 432

show controllers pse tcam summary command, 155
show environment led command, 155
show gsp groups location command, 38-39
show gsp stats client location command, 37
show install active summary command, 87
show install detail command, 76-78
show install inactive command, 87
show install log command, 87
show install log from command, 84-85
show install request command, 87
show install summary command, 76
show interfaces command, 155
show isis database detail command, 233-235
show isis interface command, 238, 241
show isis neighbor detail command, 242
show logging command, 140
show lpts pifib hardware police location command, 155
show mirror command, 94
show mpls forwarding command, 296-298
show mpls forwarding prefix command, 305
show mpls label table command, 298
show mpls ldp discovery command, 343
show mpls lsd applications command, 295
show mrib route command, 365, 367
show ospf command, 229
show ospf standby command, 224
show ospf standby database command, 223
show ospf tag, 222
show pim interface command, 365
show pim rpf command, 367, 382
show pim topology command, 366-369
show placement policy program [bgp] instance command, 45
show placement program all command, 43-45
show platform command, 76, 155, 389-394
show process bfd detail location all command, 228
show process blocked command, 147
show process boot location command, 27
show process bpm command, 248
show process command, 147
show process eigrp command, 208
show process instcmd command, 68
show process instdir command, 69-70
show process location command, 29-30
show process pidin command, 22-23
show process pidin location command, 24
show process rip command, 199
show process threadname command, 31, 148
show processes blocked location command, 25-26
show processes isis location all command, 239
show processes threadname 120 command, 18
show redundancy command, 155
show rollback points command, 130
show route summary command, 164
show run multicast-routing command, 380
show run router bgp command, 250
show running-config command, 117, 197-198, 228, 392, 419

show running-config router ospf command, 224
show sdr summary command, 385, 394
show ssh session detail command, 174, 177
show sysdb registration edm job location command, 50
show sysdb registrations notification command, 49-50
show sysdb registrations verification command, 49
show system backup verify command, 90
show system verify command, 151, 153-154
show watchdog memory-state location all command, 155
show watchdog threshold memory defaults location command, 149
task group creation, 163
user group creation, 163

shutdown command, IS-IS interface state configuration, 238

SIF (subnetwork independent functions), 232

single-module (vertical) cabling, CRS-1 multishelf connections, 409-412

single-topology command, IS-IS configuration, 233

slot allocation, DRP, 389

SM (Sparse Mode) protocol, 359, 362-374

SMU (software maintenance upgrades), 67
config-registers, verifying, 96
downloading, 61-63
install deactivate command, 85
installing, 67
MD5 signatures, verifying, 95
testing installations, 96
validating, 95

SNMP (Simple Network Management Protocol)
configuring, 137
Get messages, 136
managed devices, 135
MIB, 135
NMS, 135
Set messages, 136
supported versions, 135
traps, 136-137
VRF instances, configuring in, 138

SNMP agents, 135

snmp-server host command, 137

software
authentication, SAM commands, 95
installing, verifying installations, 76-78
patches, carrier-grade NOS, 6
process restartability
carrier-grade NOS, 6
Cisco IOS XR, 10
collaborators, 10
security, 159-160
upgrades, carrier-grade NOS, 6

SPA (shared port adapters), OIR, 123-126

speakers (BGP), 248, 282-286

sporadic scheduling, 21

SPT (Shortest Path Trees), multicast routing, 359

spt-threshold infinity command, PIM configuration, 378

SSH (Secure Shell), router access security, 173-177

SSM (Source Specific Multicast), 374-379

standby RP
booting, 82
OSPFv2, verifying in, 221-223
resetting, troubleshooting, 91

start on config (processes), 30
startup configuration, commit operation failures, 116-117
startup files
item tokens, 28
level tokens, 27
mandatory tokens, 28
name tokens, 27
path tokens, 27
process attributes, 27
static routing, CE-PE, 334
static RP, multicast routing configuration, 378-379
stations (Level 1 routers), 232
strict uRPF (Unicast Reverse Path Forwarding), 182
stub areas (OSPF), 212
subtrees, SysDB, 108
summary command, 84
supported SNMP versions, 135
swap and push label operation (MPLS), 296
swap label operation (MPLS), 295
switch fabric, down flags list, 445-446
switchover (cutover) process, 202
sync command, 438
synchronizing kernels, 9
IPC, 23
mutex, 24
semaphore, 24
shared memory space, 23
synchronous IPC, 31-32
sysadmin group, 162
SysDB (System Database)
Cisco IOS XR installations, 70
commit command, 47
configuring, 47-48
functions of, 46
processes, 47
server processes, 108
show sysdb registration edm job location command, 50
show sysdb registrations notification command, 49-50
show sysdb registrations verification command, 49
subtrees, 108
tuples, 108
syslog
best practices, 154
destination, configuring, 139-140
logging buffer, configuring, 140
messages, 138
archiving, 140-141
severity levels, 139
Syslog Event Detector, 142
system backup disk1 command, 90
system manager (sysmgr)
functions of, 26-27
processes
atttributes of, 27, 30
CLI, 29-31
core files, 30
executable paths, 30
instances, 30
JID, 28-30
last started date and time timestamp, 30
lifecycle of, 28
mandatory processes, 31
max spawns per minute, 30
PID, 28-30
respawn counts, 30
start on config, 30
state of, 30
TID, 30
System Manager Event Detector, 142

T

tables (data), BCDL, 40-41
tacacs server host command, 172
TACACS+ protocol, router access security, 169-172
target configuration
aborting, 122
building in two-stage commit model, 111-112
clearing, 122
commit operation, 112-113
available options, 114
confirmed option, 115
failed configuration, 115-116
configuration rollback, 130-132
ending, 122-123
exclusive sessions, 120-121
task groups
creating, 163-164
inheritance, 167-168
router access security, 162-168
TCL scripts, 143-146
TE (traffic engineering), MPLS TE
configuring, 313-317
FRR, 312
telnet ipv4 server max-servers command, 161
templates, configuring, 128-129
TFTP_FILE variable (ROMMON), 438
threads
blocked threads, displaying, 25-26
common thread states, 19
defining, 8, 18
IS-IS thread names, displaying, 31
priority inheritance, 20
priority inversion, 20
scheduling, 19
FIFO scheduling, 21
round-robin scheduling, 21-23
sporadic scheduling, 21
semaphore, 24
show processes threadname 120 command, 18
three-stage fabric architectures, 404, 407
throttle command, OSPF, 229
TID (thread IDs), 30
Timer Services Event Detector, 142
timers
BGP, 286-288
BGP GR, 282
IS-IS timers, 239
OSPF timers, 229
timers lsa min-interval command, OSPF timer configuration, 229
transmission capacities, network evolution, 4
traps, 136-137
trigger routers, 278
troubleshooting
CRS-1 multishelf
fabric planes, 426-428
SEA links, 429-434
EIGRP, 210-211
fabric planes, CRS-1 multishelf, 426-428
IS-IS, 245
multicast routing, 380-382
OSPF, 231
RIP, 201-202
running configuration inconsistencies, 119-120
SEA, CRS-1 multishelf, 429-434
TTL (time to live) processing, MPLS, 299

TURBOBOOT variable (ROMMON), 438
c12000 platform considerations, 81
package installations, 78-81
ROMMON variable, setting, 72-73
software installations, verifying, 76-78
standby RP, booting, 82
.vm files, booting, 73-75
two-stage commit model, 110
commit operation, 112-113
available options, 114
failed configuration, 115-116
startup configuration failures, 116-117
target configuration, building, 111-112
two-stage forwarding, 12

U

UCE (Uncorrectable Cell Errors), troubleshooting multicast routing, 381
ultimate-hop popping, 294
unlabeled label operation (MPLS), 296
unlocking configuration sessions, 121
unset command, 438
upgrades
Cisco IOS XR
composite upgrade PIE (mini.pie), 82-84
disk space usage, 95-96
install audits, 88-89
install rollback feature, 85-87
reloading routers, 63
removing inactive PIE, 87-88
router configuration backups, 96
verifying PIE/SMU config-registers, 96
PIE, composite upgrade PIE (mini.pie), 65, 82-84
SMU
downloading, 61-63
install deactivate command, 85
installing, 67
testing installations, 96
validating, 95
verifying config-registers, 96
verifying MD5 signatures, 95
software, carrier-grade NOS, 6
uRPF (Unicast Reverse Path Forwarding), 181-182
user groups
creating, 163-164
inheritance, 167-168
router access security, 162-168
user-defined EEM policies, 144-146

V

verify unicast source reachable-via command, 182
verifying
BFD, OSPFv2, 227-228
config-registers, 96
disk backups, 90
EIGRP, 210-211
EIGRP process status, 208-209
IS-IS, 233-234
authentication, 243-244
BFD verification, 241-242
interface state verification, 238-239
IPFRR verification, 242
multitopology model, 237
NSF verification, 240
show isis database detail command, 235

show isis instance 1 command, 235-237
single topology model, 235-236
multiarea adjacencies, OSPFv2, 226-227
NSF, 207, 221-223
NSR, OSPFv2, 224-226
OSPFv2, 213-214
OSPFv3, 230-231
RIP, 201-202
software installations, 76-78
standby RP status, OSPFv2, 221-223
version command, IGMP configuration, 377
versions of SNMP supported, 135
vertical (single-module) cabling, CRS-1 multishelf connections, 409-412
viewing
rollback changes, 131
running configuration, 118
VLAN (Virtual Local Area Networks), VPLS, 347-353
.vm files
booting, 73-75
downloading, 61-63
VPLS (Virtual Private VLAN service), 347-353
VPN (Virtual Private Networks)
L2VPN
l2vpn xconnect command, 343
pseudo wire redundancy, 346-347
show l2vpn forwarding summary location command, 350
show l2vpn show l2vpn bride-domain brief command, 350-353
show l2vpn xconnect neighbor command, 346
VPLS, 347-353
VPWS, 340-345
L3VPN
MP-iBGP, 320-324
VRF tables, 318-320
MPLS
common show commands table, 330
connectivity options, 324-325
RD values in VPN routes, 330-333
VRF configuration, 325-330
VPWS (Virtual Private Wire Service), 340
configuring, 341-345
local switching, 344
VRF (Virtual Routing Forwarding) tables
configuring, 318-320
PE configuration, 325-330
SNMP, configuring, 138

W - X - Y - Z

warm processes, checkpoint servers, 52
warm standbys, OSPF, 221-222
watchdog restart disable command, 53
Watchdog System Event Detector, 143
WDSYSMON (Watchdog System Monitor), 149-150

XR 12000 systems, 14