



Secure Domain Router Setup on Cisco ASR 9000 Series Routers

In Cisco IOS-XR software, secure domain routers (SDRs) are a means of dividing a single physical system into multiple logically separated routers. Cisco ASR 9000 Series Aggregation Services Routers are single-shelf routers that support only one SDR per shelf; therefore, the Cisco ASR 9000 Series Routers supports only the admin plane software infrastructure of SDR with a default configuration that is loaded at router startup. Designated shelf controller (DSC) is supported for debug and show command purposes; configuration command functions are not supported. DSC in the Cisco ASR 9000 Series Router is always the active route-switch processor (RSP).

Feature History for Configuring Secure Domain Routers on Cisco IOS XR Software

Release	Modification
Release 3.7.2	This feature was supported on Cisco ASR 9000 Series Aggregation Services Routers.

Contents

- [Parameters for Secure Domain Router, page 139](#)
- [Information About Secure Domain Routers, page 140](#)
- [Default Configuration for SDRs, page 142](#)
- [Additional References, page 143](#)

Parameters for Secure Domain Router

During the Cisco ASR 9000 Series Router startup, the following SDR parameters are automatically installed.

Initial Setup

- The initial package files (PIE) that are installed on the RSP at the factory are loaded at initial router startup.
- RSP0 is the default active processor.
- DSC is the active RSP

- The backup DSC is the standby RSP
- The rack number is 0.
- The root-system username and password must be assigned as part of the initial router configuration.
- For more information on booting a router and performing initial configuration, refer to *Cisco ASR 9000 Series Aggregation Services Routers Getting Started Guide*.

Required Cards for Each SDR

- An RSP pair must be installed in Cisco ASR 9000 Series Routers for SDR.

Task ID Requirements

- You must be in a user group associated with a task group that includes the proper task IDs for SDR commands. Only show commands and debug commands are supported on Cisco ASR 9000 Series Routers.
- If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Software Version Requirements for the Cisco ASR 9000 Series Routers

- Release 3.7.2

Maximum SDR Configurations

- The Cisco ASR 9000 Series Routers supports one owner SDR, non-owner SDRs are not supported.
- Multiple SDRs, including non-owner SDRs, are not supported.

Information About Secure Domain Routers

Review the following topics before configuring secure domain routers:

- [What Is a Secure Domain Router?](#), page 140
- [Owner SDR and Administration Configuration Mode](#), page 141
- [SDR Access Privileges](#), page 141
 - [Root-System Users](#), page 141
 - [Other SDR Users](#), page 142
- [High Availability Implications](#), page 142

What Is a Secure Domain Router?

Cisco routers running Cisco IOS XR software can be partitioned into multiple, independent routers known as *secure domain routers* (SDRs). SDRs are a means of dividing a single physical system into multiple logically separated routers. SDRs perform routing functions the same as a physical router, but they share resources with the rest of the system. For example, the software, configurations, protocols, and routing tables assigned to an SDR belong to that SDR only, but other functions, such as chassis-control and switch fabric, are shared with the rest of the system. Cisco ASR 9000 Series Routers are single shelf routers, as a result, multiple shelf functions are not supported.

Owner SDR and Administration Configuration Mode

The *owner SDR* is created at system startup and cannot be removed. This owner SDR performs system-wide function. You cannot create the owner SDR because it always exists, nor can you completely remove the owner SDR, because it is necessary to manage the router. By default, all nodes in the system belong to the owner SDR.

In Cisco IOS XR the owner SDR provides access to the Administration EXEC and Administration configuration modes. Cisco ASR 9000 Series Routers do not support the Administration configuration mode; however, debug mode is supported. Only users with root-system privileges can access the Administration modes by logging in to the primary Route-Switch Processor for the owner SDR.

Administration modes are used for the following purposes:

- Create and remove additional non-owner SDRs - not supported on Cisco ASR 9000 Series Routers
- Assign nodes to the non-owner SDRs - not supported on Cisco ASR 9000 Series Routers
- View the configured SDRs in the system.
- View and manage system-wide resources and logs.

See the [“SDR Access Privileges” section on page 141](#) for more information.

SDR Access Privileges

Each SDR in a router has a separate AAA configuration that defines usernames, passwords, and associated privileges.

- Only users with root-system privileges can access the Administration EXEC and Administration configuration modes. See the [“Root-System Users” section on page 141](#) for more information.
- Users with other access privileges can access features according to their assigned privileges for a specific SDR. See the [“Other SDR Users” section on page 142](#) for more information.

For more information about AAA policies, refer to *Configuring AAA Services on Cisco ASR 9000 Series Routers* module of the *Cisco ASR 9000 Series Aggregation Services Routers System Security Configuration Guide*.

Root-System Users

Users with root-system privileges have access to system-wide features and resources. The root-system user is created during the initial boot and configuration of the router.

The root-system user has the following privileges:

- Access to Administration EXEC and Administration configuration commands.
- Ability to create other users with similar or lower privileges.
- Complete authority over the chassis.
- Ability to install and activate software packages for SDRs.
- Ability to view the following admin plane events (owner SDR logging system only):
 - Software installation operations and events.
 - System card boot operations, such as card booting notifications and errors, heartbeat-missed notifications, and card reloads.
 - Card alphanumeric display changes.

- Environment monitoring events and alarms.
- Fabric control events.
- Upgrade progress information.

Other SDR Users

Additional usernames and passwords can be created by the root-system or root-lr users to provide more restricted access to the configuration and management capabilities of the owner SDR.

Default Configuration for SDRs

By default, the configuration of a Cisco ASR 9000 Series Router is created at router startup. For detailed instructions to add and activate software packages, see the “Managing Cisco IOS XR Software Packages” module of the *Cisco ASR 9000 Series Routers Getting Started Guide*.

Default Software Profile for SDRs

When a new SDR is created, the nodes assigned to that SDR are activated with the default software package profile. In Release 3.7.2, the default software profile is defined by the last install operation.

To view the default software profile, use the **show install active summary** command in Administration EXEC mode.

```
RP/0/RSP0/CPU0:router(admin)# show install active summary
```

```
Default Profile:
```

```
SDRs:
```

```
Owner
```

```
Active Packages:
```

```
disk0:asr9k-mpls-3.7.2.15I
```

```
disk0:asr9k-mgbl-3.7.2.15I
```

```
disk0:asr9k-mcast-3.7.2.15I
```

```
disk0:asr9k-k9sec-3.7.2.15I
```

```
disk0:asr9k-fpd-3.7.2.15I
```

```
disk0:comp-asr9k-mini-3.7.2.15I
```



Note

For detailed instructions to add and activate software packages, see the “Managing Cisco IOS XR Software Packages” module of the *Cisco ASR 9000 Series Routers Getting Started Guide*. See also the *Software Package Management Commands on Cisco ASR 9000 Series Routers* module of the *Cisco ASR 9000 Series Aggregation Services Routers System Management Command Reference*.

High Availability Implications

The following sections describe various high availability implications:

- [Fault Isolation, page 142](#)

Fault Isolation

Because the CPU and memory of an SDR are not shared with other SDRs, configuration problems that cause out-of-resources conditions in one SDR do not affect other SDRs.

Password: `xxxxxx`

Additional References

The following sections provide references related to SDR configuration.

Related Documents

Related Topic	Document Title
SDR command reference.	<i>Secure Domain Router Commands on Cisco ASR 9000 Series Routers</i> module of <i>Cisco ASR 9000 Series Aggregation Services Routers Management Command Reference Guide</i>
Initial system bootup and configuration information for a router using the Cisco IOS XR software.	<i>Cisco ASR 9000 Series Aggregation Services Routers Getting Started Guide</i>
Cisco IOS XR master command reference	<i>Cisco IOS XR Master Commands List</i>
Information about user groups and task IDs	<i>Configuring AAA Services on Cisco ASR 9000 Series Routers</i> module of <i>Cisco ASR 9000 Series Aggregation Services Routers System Security Configuration Guide</i>
Cisco IOS XR interface configuration commands	<i>Cisco ASR 9000 Series Aggregation Services Routers Interface and Hardware Component Command Reference</i>
Information about AAA policies, including instructions to create and modify users and username access privileges.	<i>Configuring AAA Services on Cisco IOS XR Software</i> module of <i>Cisco IOS XR System Security Configuration Guide</i> ,

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport