

High Availability Configuration Guide, Cisco IOS XE 17 (Cisco ASR 900 Series)

First Published: 2019-11-30

Last Modified: 2025-07-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Feature History** 1

CHAPTER 2 **High Availability Overview** 3

- Hardware Redundancy Overview 3
- Stateful Switchover 4
  - SSO-Aware Protocol and Applications 4
- Bidirectional Forwarding Detection 5

CHAPTER 3 **Installing and Upgrading Software** 7

- Software Packaging on the Router 7
  - Software Package Modes 7
  - Understanding Software Packages 8
- Provisioning Files 8
- File Systems on the Router 8
- System Requirements 9
  - RP Memory Recommendations 9
  - ROMMON Version Requirements 12
  - Determining the Software Version 12
- Autogenerated Files and Directories 12
- Setting the Router to Boot in Sub-Package Mode 13
- ISSU Support Matrix 14
  - Restrictions 17
  - Setting the Interface Module Delay for ISSU 17
- Downloading an Image 19
- Performing a Single Command Software Upgrade 19
  - Preparing for Installation 19

Completing the Single Command Upgrade 20
Performing Step-by-Step ISSU Upgrade 22
Software Upgrade Process Using Install Commands 23
Upgrading Software Using Step-By-Step Workflow 23
Upgrading Software Using Single-Step Workflow 24
Performing Single-Step Workflow 25
Tracking Software Upgrade 25
Upgrading the ROMMON on the RSP3 Module 26
Example: Verifying ROMMON Upgrade for RSP3 Module 28
Upgrading the ROMMON on the RSP Module 29
Example: Verifying ROMMON Upgrade 32
Verifying the Upgrade 32
Example: Single Command Software Upgrade for RSP3 Module 32
Example: Single Command Software Upgrade 43
Fast Booting the RSP3 .bin Image 50
Additional References 50

CHAPTER 4 **Configuring Stateful Switchover 53**
Prerequisites for Stateful Switchover 53
General Prerequisites 53
SNMP for Stateful Switchover Prerequisites 54
Restrictions for Stateful Switchover 54
General Restrictions for SSO 54
Configuration Mode Restrictions 54
Switchover Process Restrictions 54
Cisco ASR 903 Series Aggregation Services Routers Restrictions 54
SNMP for Stateful Switchover Restrictions 55
Information About Stateful Switchover 55
SSO Overview 55
Redundancy Modes 57
Stateful Switchover Mode 57
Route Processor Synchronization 57
Bulk Synchronization During Initialization 58
Incremental Synchronization 58

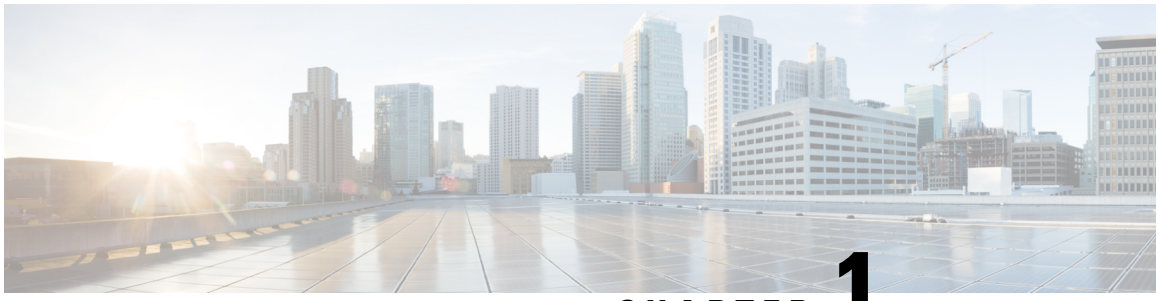
Switchover Operation 59
Switchover Conditions 59
Switchover Time 59
Core Dump Operation 59
SSO-Aware Protocols and Applications 60
Line Protocols 60
Quality of Service 62
IPv6 Support for Stateful Switchover 62
Line Card Drivers 62
Routing Protocols and Nonstop Forwarding 63
Network Management 63
Enhanced SNMP Support for High Availability 64
SNMP for Stateful Switchover Overview 64
Network Management for SSO 64
Uninterrupted Service Using SSO 64
Communication with the NMS 65
Counters and Statistics 65
Switchover Notification 65
Traps 65
SSO MIB Support 65
CISCO-RF-MIB Modifications for SSO Support 66
New cRFHistorySwitchOverTable Table in CISCO-RF-MIB for SSO Support 66
New Objects in CISCO-RF-MIB for SSO Support 66
How to Configure Stateful Switchover 67
Copying an Image onto an RP 67
Setting the Configuration Register and Boot Variables 68
Configuring SSO 69
Verifying SSO Configuration 70
Troubleshooting Stateful Switchover 71
Troubleshooting SSO 71
Troubleshooting SNMP for Stateful Switchover 72
Configuration Examples for Stateful Switchover 73
Example Configuring SSO 73
Example Verifying that SSO is Configured 73

Example Verifying Redundancy-Related States 74
Example Verifying Redundancy-Aware Protocols and Applications 74

CHAPTER 5 **Configuring Nonstop Forwarding** 77
Prerequisites for Nonstop Forwarding 77
Restrictions for Nonstop Forwarding 78
General Restrictions 78
BGP NSF Restrictions 78
EIGRP NSF Restrictions 78
OSPF NSF Restrictions 78
Information About Nonstop Forwarding 79
Nonstop Forwarding 79
Cisco NSF Routing and Forwarding 80
Cisco Express Forwarding and NSF 80
BGP NSF Operations 80
EIGRP NSF Operations 81
IPv6 support for NSF Operations 82
Nonstop Forwarding and Graceful Restart for MP-BGP IPv6 Address Family 82
Nonstop Forwarding for IPv6 RIP 82
Nonstop Forwarding for Static Routes 82
IS-IS NSF Operations 82
IETF IS-IS Configuration 83
Cisco IS-IS Configuration 83
NSF-OSPF Operations 84
How to Configure Nonstop Forwarding 84
Configuring and Verifying BGP NSF 84
Configuring and Verifying EIGRP NSF 85
Configuring NSF-OSPF 86
Configuring Cisco NSF-OSPF 87
Configuring IETF NSF-OSPF 88
Configuring and Verifying IS-IS NSF 89
Troubleshooting Nonstop Forwarding 90
Configuration Examples for Nonstop Forwarding 92
Example NSF-Capable CEF 92

Example BGP NSF 93
Example: EIGRP NSF 93
Example: Configuring Cisco NSF-OSPF 94
Example: Configuring IETF NSF-OSPF 94
Example IS-ISNSF 95
Additional References 96

CHAPTER 6 Performing an In Service Software Upgrade 99

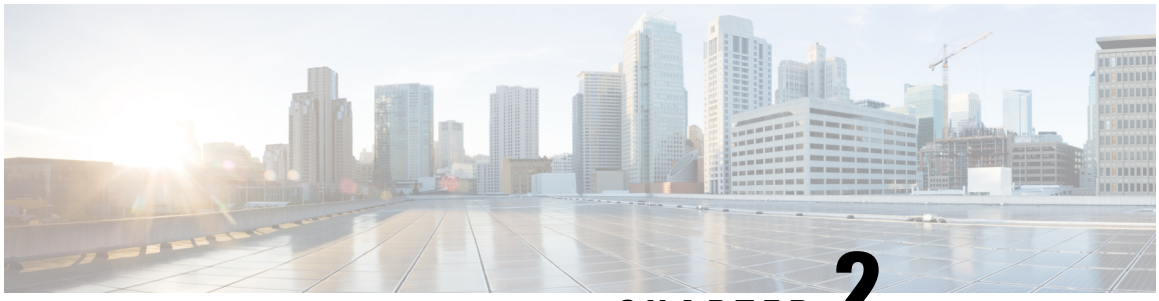


CHAPTER 1

Feature History

The following table lists the new and modified features supported in the High Availability Configuration Guide on Cisco IOS XE 17.

Feature	Description
Cisco IOS XE Bengaluru 17.6.1	
Secure eUSB Configuration	Use the **platform secure-cfg** command to provide enhanced security to the routers.
Cisco IOS XE Bengaluru 17.4.1	
Secondary ROMMON Partition Auto Upgrade	This feature supports secondary ROMMON partition auto upgrade after a successful primary ROMMON partition is complete.
Cisco IOS XE Amsterdam 17.3.1	
Fast Booting the RSP3 .bin Image	A new command **platform fastboot** is introduced on the RSP3 module. When enabled on the RSP3 module that is pre-booted with .bin image, on the next reboot, the ROMMON boots up with the corresponding packages.conf image. Boot up from the packages.conf image is much faster and thus, the boot time is reduced approximately by six to eight minutes.



CHAPTER 2

High Availability Overview

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

The unique hardware and software architecture of the router is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario.

This chapter covers the aspects of High Availability that are unique to the router. It is not intended as a comprehensive guide to High Availability, nor is it intended to provide information on High Availability features that are available on other Cisco routers that are configured and implemented identically on the router. The Cisco IOS feature documents and guides should be used in conjunction with this chapter to gather information about High Availability-related features that are available on multiple Cisco platforms and work identically on the router.

- Hardware Redundancy Overview, on page 3
- Stateful Switchover, on page 4
- Bidirectional Forwarding Detection, on page 5

Hardware Redundancy Overview

The router supports redundant Route Switch Processors (RSPs) and power supplies. Redundancy is not supported on interface modules.

Note Some interface modules require a reload during a software upgrade, briefly interrupting traffic.

Note Route Processor Redundancy (RPR) is *not* supported on the router. Stateful Switchover (SSO) is supported. See Stateful Switchover, on page 4.

Hardware redundancy provides the following benefits:

- A failover option—If a processor fails, the standby processor immediately becomes the active processor with little or no delay. The failover happens completely within the same router, so a second standby router is not needed.

- No downtime upgrades—Using features like ISSU, a software upgrade can be handled on the standby processor while the active processor continues normal operation.

Table 1: Hardware Redundancy Overview

Hardware	Support for Dual Hardware Configuration	Failover Behavior
Route Switch Processor	Yes	If an active RSP experiences an event that makes it unable to forward tra as a hardware failure, a software failure, an OIR, or a manual switch) and RSP is configured, the standby RSP immediately becomes the active RS **Note** The dual RSP reaches the STANDBY HOT state even if the system imag different on Active and Standby modules, as long as they are ISSU comp This is not applicable on the RSP3 module.
Interface module	No	No standby configurations are available for interface modules. If an interfac fails, it cannot forward traffic. In the event of an interface module shutdown, all other interface module fully operational.

Stateful Switchover

The Stateful Switchover (SSO) feature takes advantage of processor redundancy by establishing one of the processors as the active processor while the other RSP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RSP state information between the dual processors.

Stateful Switchover is particularly useful in conjunction with Nonstop Forwarding. SSO allows the dual processors to maintain state at all times, and Nonstop Forwarding lets a switchover happen seamlessly when a switchover occurs.

It is important to note that in most cases, SSO requires less downtime for switchover and upgrades than RPR. RPR should only be used when there is a compelling reason to not use SSO.

For additional information on NSF/SSO, see the Cisco Nonstop Forwarding document.

SSO-Aware Protocol and Applications

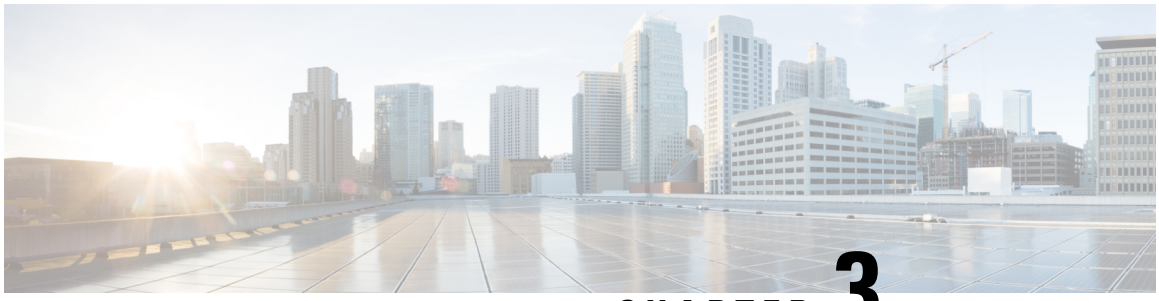
SSO-supported line protocols and applications must be SSO-aware. A feature or protocol is SSO-aware if it maintains, either partially or completely, undisturbed operation through an RSP switchover. State information for SSO-aware protocols and applications is synchronized from active to standby to achieve stateful switchover for those protocols and applications.

The dynamically created state of SSO-unaware protocols and applications is lost on switchover and must be reinitialized and restarted on switchover.

To see which protocols are SSO-aware on your router, use the following commands **show redundancy client** or **show redundancy history**.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.



CHAPTER 3

Installing and Upgrading Software

- Software Packaging on the Router, on page 7
- Provisioning Files, on page 8
- File Systems on the Router, on page 8
- System Requirements, on page 9
- Autogenerated Files and Directories, on page 12
- Setting the Router to Boot in Sub-Package Mode, on page 13
- ISSU Support Matrix, on page 14
- Downloading an Image, on page 19
- Performing a Single Command Software Upgrade, on page 19
- Performing Step-by-Step ISSU Upgrade, on page 22
- Software Upgrade Process Using Install Commands, on page 23
- Upgrading the ROMMON on the RSP3 Module, on page 26
- Upgrading the ROMMON on the RSP Module, on page 29
- Verifying the Upgrade, on page 32
- Fast Booting the RSP3 .bin Image, on page 50
- Additional References, on page 50

Software Packaging on the Router

Software Package Modes

The router can be booted using any of the following:

- Consolidated—A single software image containing a full collection of software packages. This mode provides a simplified installation and can be stored in the bootflash, a TFTP server, or a network server.
- Sub-package—One or more sub-images that are extracted from the consolidated image. This mode provides optimized memory usage and requires that you store files in the bootflash directory.

Note The router supports both consolidated and sub-packages mode boot.

Understanding Software Packages

Table 2: Individual Sub-Packages

Sub-Package	Purpose
RPBase	Route Switch Processor (RSP) operating system
RPControl	Control plane processes between IOS process and the rest of the platform.
RPAccess	Handles security features including Secure Socket Layer (SSL) and Secure Shell (SSH)
RPIOS	Cisco IOS kernel, which is where IOS features are stored and run. **Note** Each consolidated image has a unique RPIOS package.
FP Pkg	Controls FP daemons.
IO Pkg	Controls input/output driver daemons.
LC Base	Controls basic kernel functions including runtime, initialization scripts, and chassis control daemons.

Provisioning Files

Provisioning files manage the boot process when the router is configured to boot in sub-packages. The provisioning file manages the bootup of each individual sub-package. Provisioning files are extracted automatically when individual sub-package files are extracted from a consolidated package. Provisioning files are not necessary for running the router using the complete consolidated package.

File Systems on the Router

Table 3: File Systems

File System	Description
bootflash:	The boot flash memory file system on the active RSP.
cns:	The Cisco Networking Services file directory.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
stby-bootflash:	The boot flash memory file system on the standby RSP.
stby-harddisk:	The hard disk file system on the standby RSP.
stby-usb0:	The Universal Serial Bus (USB) flash drive file systems on the standby RSP. **Note** stby-usb1: is an internal port.

File System	Description
system:	The system memory file system, which includes the running configuration.
tar:	The archive file system.
tmpsys:	The temporary system files file system.
usb0:	The Universal Serial Bus (USB) flash drive file systems on the active RSP. **Note** usb1: is an internal port.

If you see a file system not listed in the above table, enter the **?** help option or see the **copy** command reference for additional information on that file system.

System Requirements

RP Memory Recommendations

Table 4: Memory Recommendations for the Cisco ASR 903 RSP1 Module - Consolidated Package Image

Platform	Image Name	Software Image	Individual Sub-package Contents	DRAM Memory
ASR 903 RSP1 Module	Cisco ASR 903 Series RSP1 UNIVERSAL W/O CRYPTO	asr903rsp1-universal.*version* .bin	asr903rsp1-rpbase.*version* .pkg	2 GB (RSP1) 4 GB (RSP1+)
			asr903rsp1-rpcontrol.*version* .pkg	
			asr903rsp1-rpaccess.*version* .pkg	
			asr903rsp1-rpios-universal.*version*. pkg	
			asr903rsp1-espbase.*version.pkg*	
			asr903rsp1-sipbase.*version* .pkg	
			asr903rsp1-sipspa.*version* .pkg	
			asr903rsp1-packages-universal. version.conf	
			packages.conf	

Platform	Image Name	Software Image	Individual Sub-package Contents	DRAM Memory
ASR 903 RSP1 Module	Cisco ASR 903 Series RSP1 UNIVERSAL NPE	asr903rsp1-universalk9_npe.*version* .bin	asr903-hw-programmables.*version* . pkg	2 GB (RSP1) 4 GB (RSP1+)
			asr903rsp1-espbase.*version* .pkg	
			asr903rsp1-packages-universalk9.*version* .pkg	
			asr903rsp1-rpacess.*version* .pkg	
			asr903rsp1-rpbase.*version* .pkg	
			asr903rsp1-rpcontrol.*version* .pkg	
			asr903rsp1-rpios-universalk9_npe.*version* .pkg	
			asr903rsp1-sipbase.*version*.pkg	
			asr903rsp1-sipspa.*version*.pkg	
			packages.conf	

Table 5: Memory Recommendations for the Cisco ASR 903 RSP2 Module - Consolidated Package Image

Platform	Image Name	Software Image	Individual Sub-package Contents
ASR 903 RSP2 Module	Cisco ASR 903 Series RSP2 UNIVERSAL W/O CRYPTO	asr900rsp2-universal.*version* .bin	asr900rsp2-rpbase.*version* .pkg
			asr900rsp2-rpcontrol.*version* .pkg
			asr900rsp2-rpaccess.*version* .pkg
			asr900rsp2-rpios-universal.*version*. pkg
			asr900rsp2-espbase.*version.pkg*
			asr900rsp2-sipbase.*version* .pkg
			asr900rsp2-sipspa.*version* .pkg
			asr900rsp2-packages-universal. version.conf
			packages.conf

Platform	Image Name	Software Image	Individual Sub-package Contents
ASR 903 RSP2 Module	Cisco ASR 903 Series RSP2 UNIVERSAL NPE	asr900rsp2-universalk9_npe.*version* .bin	asr900-hw-programmables.*version* . pkg
			asr900rsp2-espbase.*version* .pkg
			asr900rsp2-packages-universalk9.*version* .pkg
			asr900sp2-rpacess.*version* .pkg
			asr900rsp2-rpbase.*version* .pkg
			asr900rsp2-rpcontrol.*version* .pkg
			asr900rsp2-rpios-universalk9_npe.*version* .pkg
			asr900rsp2-sipbase.*version*.pkg
			asr900rsp2-sipspa.*version*.pkg
			packages.conf

Table 6: Memory Recommendations for the Cisco ASR 900 RSP3 Module - Consolidated Package Image

Platform	Image Name	Software Image	Individual Sub-package Contents
ASR 900 RSP3 Module	Cisco ASR 900 Series RSP3 UNIVERSAL W/O CRYPTO	asr900rsp3-universal.*version* .bin	asr900rsp3-rpbase.*version* .pkg
			asr900rsp3-rpcontrol.*version* .pkg
			asr900rsp3-rpaccess.*version* .pkg
			asr900rsp3-rpios-universal.*version*. pkg
			asr900rsp3-espbase.*version.pkg*
			asr900rsp3-sipbase.*version* .pkg
			asr900rsp3-sipspa.*version* .pkg
			asr900rsp3-packages-universal. version.conf
			packages.conf

Platform	Image Name	Software Image	Individual Sub-package Contents
ASR 900 RSP3 Module	Cisco ASR 900 Series RSP3 UNIVERSAL NPE	asr900rsp3-universalk9_npe.*version* .bin	asr900-hw-programmables.*version* . pkg
			asr900rsp3-espbase.*version* .pkg
			asr900rsp3-packages-universalk9.*version* .pkg
			asr900rsp3-rpacess.*version* .pkg
			asr900rsp3-rpbase.*version* .pkg
			asr900rsp3-rpcontrol.*version* .pkg
			asr900rsp3-rpios-universalk9_npe.*version* .pkg
			asr900rsp3-sipbase.*version*.pkg
			asr900rsp3-sipspa.*version*.pkg
			packages.conf

ROMMON Version Requirements

We recommend you to upgrade the ROMMON version to 15.6(33r)S.

For more information on the ROMMON package, see Cisco Software Download.

Determining the Software Version

You can use the **show version installed** command to list the installed sub-packages on the router.

Autogenerated Files and Directories



Caution Any autogenerated file in the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by customer support; altering these files can have unpredictable consequences for system performance.

Table 7: Autogenerated Files

File or Directory	Description
crashinfo files	A crashinfo file may appear in the bootflash: file system. Crashinfo files are useful for tuning and troubleshooting, but are not related to router operations: you can erase them without impacting the router's performance.

File or Directory	Description
core files	The bootflash/core directory is the storage area for .core files. **Warning** Do not erase or move the core directory.
lost+found directory	This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.
tracelogs files	The storage area for trace files is bootflash/tracelogs. Trace files are useful for troubleshooting; you can access trace files using diagnostic mode to gather information related to the IOS failure. **Warning** Do not erase or move the tracelog directory.

Setting the Router to Boot in Sub-Package Mode

Note For instructions on how to download an image file, see Downloading an Image, on page 19. In the following example, the image is located in the bootflash: Image/image-name.

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **config-register**

Example:

```
Router(config)# config-register 0x2
```

Sets the configuration register so that the router boots using a specified image in NVRAM.

Step 3 **exit**

Example:

```
Router(config)#exit
```

Exits configuration mode and returns to the EXEC command interpreter prompt.

Step 4 **request platform software package expand file** *source-URL* [**to***destination-URL*] [**force**] [**verbose**] [**wipe**]

Example:

```
Router# request platform software package expand file
stby-bootflash:Image/asr903rsp1-adventerprisek9.base.bin
```

Expands the consolidated image file on the standby RSP.

Note
This step applies only if your router has a redundant RSP.

Step 5 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 6 **boot system flash** [**flash-fs:**] [*partition-number:*] [*filename*]

Example:

```
Router(config)# boot system bootflash:Image/packages.conf
```

Sets the router to boot using the packages.conf file.

Step 7 **exit**

Example:

```
Router(config)#exit
```

Exits configuration mode and returns to the EXEC command interpreter prompt.

Step 8 **copy running-config startup-config**

Example:

```
Router# copy running-config startup-config
```

Saves the configuration.

Step 9 **reload**

Example:

```
Router#reload
```

Reloads the router.

ISSU Support Matrix

Legend:

NA: Not Applicable

NS: Not Supported

Table 8: ISSU Support Matrix

	Supported ISSU Upgrade Or Downgrade Version													
Base IOS Version	16.6.1	16.6.X (X = 2 to 6)	16.6.X (X = 7 and later)	16.9.X (X=1,2)	16.9.X (X= 3 and later)	16.11.X (X = 1 and later)	16.12.X (X= 1 and later)	17.3.1[5]	17.5.1	17.6.1	17.7.1	17.8.1	17.9.X (X=2 to 6)	17.12.X (X=2 to 5)
16.6.1	NA	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS
16.6.X (X=2 to 6)	NS	Yes	Yes	Yes[1]	Yes	Yes[11]	Yes	Yes	Yes [3 1]	Yes [3 1]	Yes [3 1]	Yes [3 1]	Yes [3 1]	Yes [3 1]
16.6.X (X=7 and later)	NS	Yes	Yes	Yes[1]	Yes	Yes[3]	Yes	Yes[3]	Yes	Yes	Yes	Yes	Yes	Yes
16.9.X (X = 1-2)	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]	Yes [3]	Yes [3]	Yes [3]	Yes [3]	Yes [3]	Yes [3]
16.9.X (X = 3 and later)	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16.11.X (X = 1 and later)	NS	Yes	Yes	Yes	Yes	NA	Yes	Yes[32]	Yes [3 4]	Yes [3 4]	Yes [3 4]	Yes [3 4]	Yes [3 4]	Yes [3 4]
16.12.1	NS	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
17.3.X (X = 2 to 8)[3]	NS	NS	NS	NS	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes
17.5.1	NS	NS	NS	NS	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes
17.6.X (X = 2 to 8)[4]	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes
17.7.1	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes
17.8.1	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes

	Supported ISSU Upgrade Or Downgrade Version													
17.9.X (X=2 to 6)	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes
17.12X (X=2 to 5)	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA

[1] Step ISSU (upgrade) to 17.1.1 with any of these images as intermediate image (16.9.3 and higher)
[2] Step ISSU (upgrade) to 17.x.x with any of these images as intermediate image (16.12.3)
[3] The 17.3.1 image auto ROMMON upgrade enables the RSP for an additional reset during software upgrade if the RSP does not have the latest ROMMON version.

For more information, see

Upgrading the Software on the Cisco ASR 900 Series Routers

[4] The 17.6.1 image auto ROMMON upgrade enables the RSP for an additional reset during software upgrade if the RSP does not have the latest ROMMON version.

For more information, see

Upgrading the Software on the Cisco ASR 900 Series Routers

Note

- All phase 1 interface modules undergo FPGA upgrade during the ISSU to Cisco IOS XE 17.4.1 from any earlier releases. This impacts the traffic for that IM until the FPGA is upgraded and the IM comes up after reload.
- All phase 1 and phase 2 interface modules undergo FPGA upgrade during ISSU to Cisco IOS XE 17.8.1 from any earlier releases in RSP2 and RSP3. This impacts the traffic for that interface module until the FPGA is upgraded and the interface module comes up after reload.
- For the phase 1 interface module nodes which are ISSU upgraded from Cisco IOS XE 17.4.1 or later release to Cisco IOS XE 17.8.1, the traffic is not impacted.

  Refer the following table for supported IMs:

Table 9: ASR 900 Supported Ethernet Interface Module

Phase 1 IM	Phase 2 IM	Phase 3 IM
A900-IMA8S	A900-IMA8S1Z	A900-IMA8Z
A900 -IMA8T	A900-IMA8T1Z	A900-IMA2F
A900-IMA1X	A900-IMA2Z	A900-IMA2C

Restrictions

- The ISSU upgrade operation requires that the ROMmon version be 15.6(33r)S or higher for all releases starting from release Cisco IOS XE 16.11.x. For Cisco IOS XE Releases 16.6.x to 16.9.x, the minimum ROMmon version must be 15.6(20r)S.
- You must enable the **port-channel max-memlink-per-pc 8** command when downgrading from Cisco IOS XE Release 16.11.x else, ISSU will fail.
- For Cisco IOS XE Releases from 17.12.x, for ISSU upgrade, there's an increase in the ISSU upgrade duration when CEM scale on the IM is enabled for 5000 or more services.
- Executing service-related commands, including show commands, during an ISSU upgrade or IM reload may lead to unpredictable outcomes. We recommend to wait until the upgrade or reload process has fully completed before running these commands.

Setting the Interface Module Delay for ISSU

Interface module delay refers to the duration that the system waits before enabling the new software on the upgraded interface modules. This delay is to ensure that all the interface modules have successfully synchronized with the new software before they are functioning.

The delay duration can vary depending on several factors, including the specific network device, the number of interface modules, and the complexity of the software upgrade being performed.

To set an optimum delay duration for the ISSU process, refer to the following table:

Interface Module	CEM FPD upgrade		FPD Upgrade (Seconds)	CEM & FPD Upgrade	
	CEM Scale	Upgrade Time (Seconds)		CEM Scale	Upgrade Time (Seconds)
A900-IMA48D-C	256	120	NA	256	240
	512	180		512	300
A900-IMA48T-C	672	180	NA	672	300
	1344	360		1344	480
A900-IMA3G-IMSG	672	300	NA	672	420
	1344	360		1344	480
A900-IMA1Z8S-CXMS	100	480	NA	100	660
	500	540		500	720
	1344	660		1344	840
	2500	840		2500	1020
	5000	1200		5000	1380

Interface Module	CEM FPD upgrade		FPD Upgrade (Seconds)	CEM & FPD Upgrade	
	CEM Scale	Upgrade Time (Seconds)		CEM Scale	Upgrade Time (Seconds)
A900-IMA1Z8S-CX	100	420	NA	100	660
	500	420		500	720
	1344	540		1344	780
	2500	660		2500	900
	5000	900		5000	1140
A900-IMA8S	NA		62	NA	
A900- IMA8T	NA		63	NA	
A900-IMA1X	NA		88	NA	
A900-IMA8S1Z	NA		135	NA	
A900-IMA8T1Z	NA		136	NA	
A900-IMA2Z	NA		133	NA	
A900-IMA2F	NA		318	NA	
A900-IMA8Z	NA		406	NA	
A900-IMA1C	NA		328	NA	
A900-IMA2C	NA		330	NA	
A900-IMA8CS1Z-M	NA		405	NA	

For example, consider a router with four interface modules:

- A900-IMA48D-C with 512 CEM FPD upgrade
- A900-IMA1Z8S-CXMS with 1344 CEM FPD upgrade
- A900-IMA8CS1Z-M with FPD upgrade
- A900-IMA8T with no FPGA upgrade

The A900-IMA8T interface module won’t reload due to no FPGA version upgrade. The remaining three interface modules reload during the ISSU process.

Compare the delay durations of the three interface modules and select the one with the longest duration. For example, the A900-IMA1Z8S-CXMS delay duration is 660 seconds, which is the longest compared to the delay durations of the other two interface modules.

Based on this information, set the delay duration to 660 seconds for the ISSU upgrade for this router.

Note For more information on FPGA versions, refer to the respective version release notes.

Downloading an Image

Download the image to the same partition of the bootflash where the base image exists. For information on downloading images see, Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S.

Note Ensure that you have chosen an upgrade image that is supported by your current software version.

Performing a Single Command Software Upgrade

A single command upgrade updates the active and standby RSPs with a single IOS command. Follow these steps to complete the one-shot upgrade.

Preparing for Installation

Verify the chassis is booted using sub-package mode and in hot standby state, else set the router to sub-package mode. For more information, see Setting the Router to Boot in Sub-Package Mode, on page 13.

Procedure

Step 1 Download the new image file from Cisco.com on the chassis.

Step 2 Open a console session to the active RSP.

Step 3 Copy the new consolidated image file to the active image bootflash directory such that the new image file is in the same location as the existing image file.

Note
Do not copy the packages.conf file to a new directory after expanding the package. It is required that the packages.conf file and sub package files exist in the same directory.

Note
It is not necessary to copy the new consolidated image file to the standby RSP; the one-shot upgrade process completes this step.

Step 4 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 5 **redundancy**

Example:

```
Router(config)# redundancy
Router(config-red)#
```

Enters redundancy configuration mode.

Step 6 **mode sso**

Example:

```
Router(config-red)# mode sso
```

Sets the router in SSO redundancy mode.

Step 7 **end**

Example:

```
Router(config)# end
```

Exits configuration mode and returns to the EXEC command prompt.

Step 8 Confirm that the router has reached SSO state

Example:

```
*Jan 12 17:52:26.516: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
```

Wait for the output before proceeding.

Step 9 **copy running-config startup-config**

Example:

```
Router# copy running-config startup-config
```

Saves the configuration.

Completing the Single Command Upgrade



Note Do *not* press CTRL+C when the single command upgrade is in process. The system shall reach the command prompt only after successful completion of the upgrade.

Note The Ethernet interface and TDM IM modules may reset, when firmware changes with the IOS image. The following TDM interface modules reset during the upgrade, irrespective of firmware changes with the IOS image:

- Cisco ASR 900 8 port RJ48C T1/E1 Interface Module
- Cisco ASR 900 16-Port T1/E1 Interface Module
- Cisco ASR 900 32-Port T1/E1 Interface Module
- Cisco ASR 900 Series 4-Port OC3/STM-1 or 1-Port OC12/STM-4 Module

Procedure

Step 1 (Optional) **platform issu reload interface-module sequence** *sequence of all IMs*

Reloads the interface modules in a sequence. Separate the IM numbers with a single space. If there are 16 IMs, sequence for all 16 IMs should be given, irrespective of the IMs being physically present or not. If the sequence is not configured using this command, the reload happens sequentially, by default.

Step 2 **request platform software package install node file** *file-URL* [**interface-module-delay** *delay*]

Example:

```
Router# request platform software package install node file
 bootflash:Image/asr903rsp1-adventerprisek9.upgrade.bin interface-module-delay 150
```

Initiates the one-shot installation procedure using the consolidated image file.

Note
You can adjust the delay between the OIR of each IM using the **interface-module-delay** keyword. We recommend you set the **interface-module-delay** value to 150 seconds or greater in order to ensure sufficient time for IM software upgrades. Keywords other than **interface-module-delay** are not supported.

Step 3 Wait for the router messages.

The router displays a series of STAGE/SUCCESS messages.

For sample output of a single command upgrade, see Example: Single Command Software Upgrade, on page 43.

Step 4 Wait for original active RSP to reboot.

The active RSP reboots and returns to the console prompt.

Step 5 Switch to the new active console.

Step 6 Wait for new active console to return to SSO state

Example:

```
*Jan 12 17:52:26.516: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
```

Confirms that the router has reached SSO state; wait for this output before proceeding.

Performing Step-by-Step ISSU Upgrade

Note Ensure that the wildcard "**-*.**" is used while installing the packages on the active RSP module (Step 8).

Procedure

Step 1 Verify the chassis is booted using sub-package mode and in hot standby state, else set the router to sub-package mode, see Setting the Router to Boot in Sub-Package Mode, on page 13.

Step 2 Download the image on the chassis.

Step 3 Extract the sub-package images from the asr903rsp1-adventerprisek9.upgrade.bin image on the active RSP using the **request platform software package expand file bootflash:Image/ asr903rsp1-adventerprisek9.upgrade.bin** command.

Step 4 Extract the sub-package image from the asr903rsp1-adventerprisek9.upgrade.bin image on the standby RSP using the **request platform software package expand file stby-bootflash:Image/asr903rsp1-adventerprisek9.upgrade.bin** command.

Step 5 Upgrade all the sub-packages on the standby RSP using the **request platform software package install rp** *stdby_slot_num* **file stby-bootflash:asr903rsp1-*.upgrade.pkg** command.

Step 6 Reload the standby module from active RP using the **hw-module slot** *stdby_slot_num* **reload** command and wait for the standby to reach Hot standby state.

Step 7 (Optional) Reload the interface modules in a sequence using the **platform issu reload interface-module sequence** *sequence of all IMs* command.

Separate the IM numbers with a single space. If there are 16 IMs, sequence for all 16 IMs should be given, irrespective of the IMs being physically present or not. If the sequence is not configured using this command, the reload happens sequentially, by default.

Step 8 Execute the **request platform software package install rp** *active_slot_num* **file bootflash:asr903rsp1-sipspa.upgrade.pkg slot** *active_slot_num* **bay** *im_slot_num* **force** command for each IM present in the router.

Note
The interface modules present are reset during the installation. Verify that the IM state is OK before proceeding to the next interface module.

Step 9 Upgrade all the sub-packages on the active RSP using the **request platform software package install rp** *active_slot_num* **file bootflash:asr903rsp1-*.upgrade.pkg** command.

Step 10 Perform a switchover. Wait for the new standby RSP module to reach hot standby state.

The latest image is upgraded on the router.

Note

If you have missed the package installation on any of the IM in Step 7 and proceeded to Step 8, the packages are automatically installed for the missed IMs. The IMs may reset if the firmware changes in Step8.

Note
ISSU from 16.9.x or 16.12.x release to 17.3.1 release and later is not supported directly. Ensure that you have the latest build and perform an ISSU from 16.9.3 release to 16.9.6 release or later, then to 17.3.1 release or later.

Software Upgrade Process Using Install Commands

Cisco ASR 900 Series Aggregation Services Routers support In-Service Software Upgrades (ISSU) procedure to upgrade the software. The *ISSU-using-install-cmds-for-RSP3* feature introduces a new method of software upgrade process by using the install command for Cisco ASR 903 Series Aggregation Services Routers.



Note Starting with Cisco IOS XE Amsterdam 17.3.1, the Install Workflow based ISSU method is supported on the Cisco RSP3 module .

Prerequisite

- Ensure that the standby RP is in the standby-hot state.
- Enable autoboot when using the install command so that the device is automatically reloaded with the configuration registry using the boot system command.

Guidelines

- Perform software upgrade process only during a maintenance window.
- Do not enable new features during a software upgrade process as it may require configuration changes.

Sub-Package Upgrade

Upgrading Software Using Step-By-Step Workflow

The step-by-step workflow involves, to add, activate, and commit the configuration. After activation, all the cards are upgraded to the new software version but does not commit automatically. You must manually commit using the install commit command. The advantage is that, it allows the system to roll back to a previous software version. The system automatically rolls back if the rollback timer is not stopped using the install abort-timer-stop command. If the rollback timer is stopped, then the new software version could be run on the device for any duration and then roll back to the previous version.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **install add file {bootflash:| tftp:}**

Example:

```
Router# install add tftp bootflash:
```

Downloads the image into the bootflash. The image is copied to the boot directory (boot_dir), the location where Route Processors (RPs) are booted.

Step 3 **install activate issu [linecard-delay seconds]**

Example:

```
Router# install activate issu
```

Provisions the standby RP with the new software and reloads with the new software version.

- linecard-delay *seconds* — Waits for a specified duration before upgrading the next slot.
- The rollback timer will be restarted.

Step 4 **install commit**

Example:

```
Router# install commit
```

Saves the configuration, performs the necessary clean-up, enables the new software as permanent (removing the older version of the software) and stops the rollback timer.

Note
There is no rollback when this command is used.

Upgrading Software Using Single-Step Workflow

The single-step workflow involves, to add, activate, and commit the configuration. Rollback is not supported, as the upgrade is committed automatically.

Rollback

You can rollback the system before a commit. You can rollback a device to the initial stage using the **install abort issu** command or after the expiry of the rollback timer before the install commit command is used. If the install commit command is used, then rollback is not allowed.

Rollback involves the following:

- Provision and reset the standby RP.
- Provision and reset the active RP.

If the rollback timer is not stopped by using the **install abort stop-timer** command, the device rolls back to an earlier software version on expiry of the rollback timer. The default value of the rollback timer is 120 minutes.

The rollback timer value can be set via the **install activate location standby auto-abort-timer seconds** command.

Performing Single-Step Workflow

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **install add file {bootflash: | tftp: } activate issu [linecard-delay seconds] commit**

Example:

```
Router# install add tftp bootflash: activate issu commit
```

Enables the standby RP with new software and triggers the standby RP to become active RP with new software version.

- linecard-delay *seconds* — Waits for a specified duration before upgrading the next slot.
- commit — Saves the configuration, performs the necessary clean-up, enables the new software as permanent (removes the older version of the software) and stops the rollback timer. Any reboot after the commit, boots with the new software. There is no rollback when this keyword is used.

Tracking Software Upgrade

You can track the ISSU progress using the **show issu state detail** command.

Upgrading the ROMMON on the RSP3 Module

Table 10: Feature History

Feature Name	Release Information	Description
Secondary ROMMON Partition Auto Upgrade	Cisco IOS XE Bengaluru 17.4.1	This feature supports secondary ROMMON partition auto upgrade after a successful primary ROMMON partition is complete.

The router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.

Note We recommend that both region ROM0 andROM1 are upgraded.

For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, and Cisco IOS XE Amsterdam 17.1.x, a minimum diskspace of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a diskspace lesser than 2 MB, ROMMON auto upgrade fails and the router reboots. This is applicable to Cisco ASR 903 and Cisco ASR 907 routers.

Routers running a ROMMON version that is lower than version 15.6(33r)S is auto upgraded to version 15.6(33r)S during a router restart.However, if a Cisco IOS XE release with ROMMON image is bundled with a version lower than the running ROMMON version, then the ROMMON is not auto downgraded.

While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON during the auto upgrade. However, the router can be reloaded during the next planned reload to complete the secondary rommon upgrade. This is applicable to ASR 903 and ASR 907 routers.

Starting with Cisco IOS XE Bengaluru Release 17.4.1, secondary ROMMON partition is auto upgraded after a successful primary ROMMON partition is complete. The router does not reload to complete the secondary ROMMON upgrade. The secondary ROMMON upgrade can be completed during planned reload of the router.

For Cisco IOS XE Gibraltar Release 16.9.4 with ROMMON release version 15.6(42r)S, ROMMON is secure. Once the ROMMON version is upgraded, it cannot be downgraded to a non-secure ROMMON version.

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Procedure

Step 1 Check the RSP bootup ROMMON region (ROM0 or ROM1). The example, shows the RSP boots up from ROM0 region.

Example:

Step 2 Copy the ROMMON image to the bootflash on the active and standby RSP.

Example:

```
copy bootflash:rsp3_rommon_156_33r_s.pkg
```

Step 3 Use the **upgrade rom-monitor filename** *bootflash:rsp3_rommon_156_33r_s.pkg* **R0** command to upgrade the version.

Note
R0 represents RSP in slot0 of the chassis. Step 3 upgrades the ROMMON region of the RSP that is not used (ROM1 region) as ROM 0 region is used (in this procedure) in Step 1 to boot up the RSP.

Step 4 Upgrade the ROMMON on the Standby RSP (for High Availability) using **upgrade rom-monitor filename** *bootflash:rsp3_rommon_156_33r_s.pkg* **R1** command.

Note
R1 represents the RSP in slot1 of the chassis. Step 4 upgrades the ROMMON region of the RSP that is not used (ROM 0 region).

Step 5 Reload the router.

Example:

```
System Bootstrap, Version 15.6(20r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2017 by cisco Systems, Inc.
Compiled Tue 23-May-17 07:20 by sabind
Starting Initialization of FMAN0
Loading ucode for FMAN0, size: 31424, ver: 106.04.14
fixup address:7ffff278 contentsoffixup:7ffff000
DCFG_CCSR_PORSR1(cfg_0_9 pins):22FB7F7F
RC Vendor ID[0x8241957]
PEX up stream Vendor ID[0x860910b5]
PEX down stream vendor ID [0x860910b5]
FPGA vendor ID[0x5f1137]
PCI Configuration done..
IOFPGA version[16040627]

Current image running: Boot ROM0
Last reset cause: RSP-Board
Rommon upgrade requested
Flash upgrade reset 1 in progress
......BootPage Setting Done - Next DDR-init

System Bootstrap, Version 15.6(33r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Sat 06-Oct-18 23:23 by pallavik
Starting Initialization of FMAN0
Loading ucode for FMAN0, size: 31424, ver: 106.04.14
fixup address:7ffff278 contentsoffixup:7ffff000
DCFG_CCSR_PORSR1(cfg_0_9 pins):22FB7F7F
RC Vendor ID[0x8241957]
PEX up stream Vendor ID[0x860910b5]
PEX down stream vendor ID [0x860910b5]
FPGA vendor ID[0x5f1137]
PCI Configuration done..
IOFPGA version[16040627]

Current image running: *Upgrade in progress* Boot ROM1
```

```
Last reset cause: BootRomUpgrade
Configuring zarlink...
We're coming up from a flash upgrade reset cookie
UEA platform with 3670016 Kbytes of main memory

We're coming up from a flash upgrade reset cookie
RSP3#
```

Step 6 Reload the router again to confirm bootup from upgraded ROMMON region ROM1.

Example:

```
System Bootstrap, Version 15.6(33r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Sat 06-Oct-18 23:23 by pallavik

Current image running: Boot ROM1
```

Step 7 Repeat Step 3 to Step 6 to update the other region on the RSP (ROM0) region in this procedure.

Example: Verifying ROMMON Upgrade for RSP3 Module

Use the show platform command to verify the ROMMON upgrade.

```
Router# show platform
RSP3#show platform
Chassis type: ASR-903

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      A900-IMA1X          ok                    00:18:41
 0/1      A900-IMA2Z          ok                    00:18:41
 0/2      A900-IMA8S1Z        ok                    00:18:40
 0/3      A900-IMA8Z          ok                    00:18:41
 0/4      A900-IMA2F          ok                    00:18:41
 0/5      A900-IMA1C          ok                    00:18:40
R0        A900-RSP3C-400-S    ok, active            00:20:48
R1        A900-RSP3C-400-S    ok, standby           00:20:48
F0                            ok, active            00:20:48
F1                            ok, standby           00:20:48
P0        A900-PWR1200-A      ok                    00:19:59
P1        Unknown             N/A                   never
P2        A903-FAN            ok                    00:19:57

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
R0        16040627            15.6(33r)S
R1        16040627            15.6(33r)S
F0        16040627            15.6(33r)S
F1        16040627            15.6(33r)S
```

Upgrading the ROMMON on the RSP Module

Table 11: Feature History

Feature Name	Release Information	Description
Secondary ROMMON Partition Auto Upgrade	Cisco IOS XE Bengaluru 17.4.1	This feature supports secondary ROMMON partition auto upgrade after a successful primary ROMMON partition is complete for NCS 4216 routers.
Secondary ROMMON Version Auto Upgrade	Cisco IOS XE Bengaluru 17.5.1	After primary ROMMON version is auto upgraded, secondary ROMMON version auto upgrade process takes place. The secondary ROMMON upgrade is only completed during the next planned manual reload of the router. This is applicable to NCS 4201/4202 routers.

Starting with Cisco IOS XE Bengaluru release, 17.6.1, the 15.6(49r)S ROMMON version filters the restricted ROMMON variables during the bootup.

Starting with Cisco IOS XE Bengaluru release, 17.5.1, secondary ROMMON partition is also auto upgraded after a successful primary ROMMON partition upgrade is complete. You can reload the router at the next planned reload to complete the secondary ROMMON upgrade.



Note If the secondary ROMMON version is lesser than that of the primary ROMMON version, the secondary ROMMON gets auto upgraded.

For Cisco IOS XE Amsterdam Release 17.3.x, Cisco IOS XE Bengaluru Release 17.4.x, and earlier, the secondary ROMMON partition is not auto upgraded. You must manually upgrade it using the **upgrade rom-mon filename** command.

Starting with ROMMON release version 15.6(43r)S, ROMMON version is secure. Once the ROMMON version is upgraded, it cannot be downgraded to a non-secure ROMMON version.

Secure ROMMON is supported from Cisco IOS XE Amsterdam Release 17.3.1 onwards. However, it is compatible with all the releases.

Any future secure ROMMON upgrade or downgrade is only possible from Cisco IOS XE Amsterdam Release 17.3.1 onwards.

Any non-secure FPGA bundled releases moving to Cisco IOS XE Bengaluru Release 17.3.x or future releases can result in an FPGA upgrade and a ROMMON upgrade. If FPGA upgrade happens parallely with the ROMMON upgrade, you can only expect a single reload. If FPGA upgrade gets delayed and happens post ROMMON upgrade, two reloads are expected to complete both the upgrade processes. This is followed by a successful bootup of the target release image.

The router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.

Note For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, Cisco IOS XE Amsterdam 17.1.x, and Cisco IOS XE Amsterdam 17.3.1, a minimum diskspace of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a diskspace lesser than 2 MB, ROMMON auto upgrade fails and the router reboots.

Note Routers running a ROMMON version that is lower than version 15.6(33r)S is auto upgraded to version 15.6(33r)S during a router restart. However, if a Cisco IOS XE release with ROMMON image is bundled with a version lower than the running ROMMON version, then the ROMMON is not auto downgraded.

Note Before installing the Cisco IOS XE Amsterdam 17.3.1, you *must* upgrade the ROMMON to version 15_6_43r_s or higher to avoid bootup failure. This is applicable to NCS 4202 routers.

Note Starting with Cisco IOS XE Amsterdam 17.3.1, While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade.

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Procedure

Step 1 Check the RSP bootup ROMMON region (ROM0 or ROM1). The example, shows the RSP boots up from ROM0 region.

Example:

```
System Bootstrap, Version 15.2(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Wed 07-Dec-11 07:33 by tinhuang
Current image running: Boot ROM0
```

Step 2 Copy the ROMMON image to the bootflash on the active and standby RSP.

Example:

```
copy bootflash:asr903-rommon.153-1r.S1.pkg
```

Step 3 Use the **upgrade rom-monitor filename** *bootflash:asr903-rommon.153-1r.S1.pkg* **R0** command to upgrade the version.

Note
R0 represents RSP in slot0 of the chassis. Step 3 upgrades the ROMMON region of the RSP that is not used (ROM1 region) as ROM 0 region is used (in this procedure) in Step 1 to boot up the RSP.

Step 4 Upgrade the ROMMON on the Standby RSP (for High Availability) using **upgrade rom-monitor filename** *bootflash:asr903-rommon.153-1r.S1.pkg* **R1** command.

Note
R1 represents the RSP in slot1 of the chassis. Step 4 upgrades the ROMMON region of the RSP that is not used (ROM 0 region).

Step 5 Reload the router.

Example:

```
System Bootstrap, Version 15.2(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Wed 07-Dec-11 07:33 by tinhuang
Current image running: Boot ROM0
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Rommon upgrade requested
Flash upgrade reset 1 in progress
.......
System Bootstrap, Version 12.2(20120514:121217) [npenumar-pegasus_rommon_02 183], DEVELOPMENT
 SOFTWARE
Copyright (c) 1994-2008 by cisco Systems, Inc.
Compiled Fri 15-Jun-12 11:45 by ccai
Current image running: *Upgrade in progress* Boot ROM1
Last reset cause: BootRomUpgrade
UEA platform with 2097152 Kbytes of main memory
```

Step 6 Reload the router again to confirm bootup from upgraded ROMMON region ROM1.

Example:

```
System Bootstrap, Version 15.2(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Fri 15-Jun-12 11:45 by ccai
Current image running: Boot ROM1
```

Step 7 Repeat Step 3 to Step 6 to update the other region on the RSP (ROM0) region in this procedure.

Note
We recommend that both region ROM0 andROM1 are upgraded.

Example: Verifying ROMMON Upgrade

Use the show platform command to verify the ROMMON upgrade.

```
Router# show platform

Chassis type: ASR-903
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      A900-IMA1X          ok                    04:48:07
 0/1      A900-IMA1X          ok                    04:43:42
 0/4      A900-IMA8T          ok                    05:18:21
 0/5      A900-IMA8T          ok                    05:18:21
R0        A903-RSP1A-55       ok, active            05:23:11
R1        A903-RSP1A-55       ok, standby         05:23:11
F0                                        ok, active            05:23:11
F1                                        ok, standby         05:23:11
P0        A900-PWR550-D       ok                    05:20:02
P1        A900-PWR550-D       ok                    05:19:55
P2        A903-FAN            ok                    05:19:45
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        11102133            15.3(1r)S1
R1        11102133            15.3(1r)S1
F0        11102133            15.3(1r)S1
F1        11102133            15.3(1r)S1
```

Verifying the Upgrade

Example: Single Command Software Upgrade for RSP3 Module

```
Router#$request platform software package install node file
bootflash:issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin interface-module-delay 150
NOTE: Currently node has booted from a provisioning file
NOTE: Going to start a dual rp sub-packages node ISSU install

--- Starting disk space verification ---
Finished disk space verification

--- Starting initial file path checking ---
Copying bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin to
stby-bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin
Finished initial file path checking

--- Starting config-register verification ---
Finished config-register verification

--- Starting image file expansion ---
Expanding image file: bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin

*Jul 26 08:03:51.807: %INSTALL-5-OPERATION_START_INFO: R0/0: packtool: Started expand package
 bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin
*Jul 26 08:05:42.842: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/5/1, changed state to
up
*Jul 26 08:05:42.843: %IOSXE_RP_ALARM-6-INFO: cleared CRITICAL TenGigabitEthernet0/5/1:
Physical Port Link Down
*Jul 26 08:05:43.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/5/1,
 changed state to up
```

```
*Jul 26 08:06:12.795: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4/6,
 changed state to up
*Jul 26 08:06:14.189: %LINK-3-UPDOWN: Interface GigabitEthernet0/4/6, changed state to up
*Jul 26 08:06:14.192: %IOSXE_RP_ALARM-6-INFO: cleared CRITICAL GigabitEthernet0/4/6: Physical
 Port Link Down
*Jul 26 08:06:14.210: %LINK-3-UPDOWN: Interface BDI500, changed state to up
*Jul 26 08:06:14.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface BDI500, changed state
 to upImage file expanded and copied
Expanding image file: stby-bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin

*Jul 26 08:09:11.903: %INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: packtool: Completed expand
 package bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin
*Jul 26 08:09:18.982: %INSTALL-5-OPERATION_START_INFO: R1/0: packtool: Started expand package
 bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.binImage file expanded and
copied
Finished image file expansion

STAGE 1: Installing software on standby RP
================================================

*Jul 26 08:14:46.426: %INSTALL-5-OPERATION_COMPLETED_INFO: R1/0: packtool: Completed expand
 package bootflash:/issu/asr900rsp3-universalk9_npe.16.12.01prd15.SPA.bin--- Starting install
 local lock acquisition on R0 ---
Finished install local lock acquisition on R0

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization


*Jul 26 08:14:49.404: %INSTALL-5-OPERATION_START_INFO: R0/0: provision: Started install
package stby-bootflash:issu/*rsp3-*16.12.01prd15.SPA*.pkg--- Starting install local lock
acquisition on R1 ---

Finished install local lock acquisition on R1



--- Starting local lock acquisition on R1 ---

Finished local lock acquisition on R1



--- Starting file path checking ---


*Jul 26 08:14:55.232: %INSTALL-5-OPERATION_START_INFO: R1/0: provision: Started install
package stby-bootflash:issu/*rsp3-*16.12.01prd15.SPA*.pkgFinished file path checking



--- Starting image file verification ---

Checking image file names

Locating image files and validating name syntax

  Found asr900rsp3-espbase.16.12.01prd15.SPA.pkg

  Found asr900rsp3-rpaccess.16.12.01prd15.SPA.pkg
```

```
  Found asr900rsp3-rpbase.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpboot.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpcontrol.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpios-universalk9_npe.16.12.01prd15.SPA.pkg
  Found asr900rsp3-sipbase.16.12.01prd15.SPA.pkg
  Found asr900rsp3-sipspa.16.12.01prd15.SPA.pkg
Verifying image file locations
Inspecting image file types
    WARNING: In-service installation of IOSD package
    WARNING: requires software redundancy on target RP
    WARNING: or on-reboot parameter
    WARNING: Automatically setting the on-reboot flag
    WARNING: In-service installation of RP Base package
    WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatibility verification ---
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
```

```
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished ISSU compatibility verification

--- Starting list of software package changes ---
Old files list:
  Removed asr900rsp3-espbase.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpaccess.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpbase.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpboot.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpcontrol.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpios-universalk9_npe.16.11.01a.SPA.pkg
  Removed asr900rsp3-sipbase.16.11.01a.SPA.pkg
  Removed asr900rsp3-sipspa.16.11.01a.SPA.pkg
New files list:
  Added asr900rsp3-espbase.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpaccess.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpbase.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpboot.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpcontrol.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpios-universalk9_npe.16.12.01prd15.SPA.pkg
  Added asr900rsp3-sipbase.16.12.01prd15.SPA.pkg
  Added asr900rsp3-sipspa.16.12.01prd15.SPA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
```

```
SUCCESS: Software provisioned.  New software will load on reboot.


*Jul 26 08:22:34.205: %INSTALL-5-OPERATION_COMPLETED_INFO: R1/0: provision: Completed install
 package stby-bootflash:issu/*rsp3-*16.12.01prd15.SPA*.pkg
*Jul 26 08:22:40.703: %INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: provision: Completed install
 package stby-bootflash:issu/*rsp3-*16.12.01prd15.SPA*.pkgSTAGE 2: Restarting standby RP
==================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby RP to reach terminal redundancy state ---

*Jul 26 08:22:51.278: %IOSXE_OIR-6-OFFLINECARD: Card (rp) offline in slot R1
*Jul 26 08:22:51.294: %IOSXE_RP_ALARM-6-INFO: asserted MAJOR module R1: Boot state
*Jul 26 08:22:51.316: %IOSXE_OIR-6-OFFLINECARD: Card (fp) offline in slot F1
*Jul 26 08:22:51.371: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Jul 26 08:22:51.371: %IOSXE_RP_ALARM-6-INFO: asserted MAJOR module R0: Secondary removed
*Jul 26 08:22:51.372: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Jul 26 08:22:51.374: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Jul 26 08:22:54.074: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Jul 26 08:22:55.376: %IOSXE_RP_ALARM-6-INFO: cleared MAJOR module R1: Boot state
*Jul 26 08:22:55.377: %IOSXE_RP_ALARM-6-INFO: asserted MAJOR module R1: Unknown state
*Jul 26 08:22:55.437: %IOSXE_OIR-6-REMCARD: Card (rp) removed from slot R1
*Jul 26 08:22:55.438: %IOSXE_RP_ALARM-6-INFO: asserted CRITICAL slot R1: RP Removed OIR
Alarm
*Jul 26 08:22:55.438: %ALARM-3-CLEAR: cleared MAJOR module R1 Unknown state
*Jul 26 08:22:55.540: %IOSXE_OIR-6-REMCARD: Card (fp) removed from slot F1
*Jul 26 08:22:55.642: %IOSXE_OIR-6-REMCARD: Card (cc) removed from slot 1
*Jul 26 08:22:55.407: %CMRP-6-FP_HA_STATUS: R0/0: cmand: F0 redundancy state is Active with
 no Standby
*Jul 26 08:22:55.412: %CMRP-6-RP_SB_RELOAD_REQ: R0/0: cmand: Reloading Standby RP: initiated
 by RF reload message
*Jul 26 08:23:06.692: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in slot R1
*Jul 26 08:23:06.693: %IOSXE_RP_ALARM-6-INFO: cleared CRITICAL slot R1: RP Removed OIR Alarm

*Jul 26 08:23:06.694: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F1
*Jul 26 08:23:06.702: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 1
*Jul 26 08:23:06.703: %IOSXE_RP_ALARM-6-INFO: asserted MAJOR module R1: Unknown state
*Jul 26 08:23:18.288: %IOSXE_RP_ALARM-6-INFO: cleared MAJOR module R1: Unknown state
*Jul 26 08:23:18.289: %IOSXE_RP_ALARM-6-INFO: asserted MAJOR module R1: Boot state
*Jun  7 22:58:01.164: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.169: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.1: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.184: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.185: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.185: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.186: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.188: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.190: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.191: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:06:00.0: of_irq_parse_pci()
 failed with rc=-22
*Jun  7 22:58:01.460: %IOSXE-3-PLATFORM: R1/0: kernel: pci 0001:0e:00.0: BAR 0: error
updating (high 0x00000f != 0x000000)
*Jun  7 22:58:01.508: %IOSXE-3-PLATFORM: R1/0: kernel: mdio_bus ffb4fc000: MDIO device at
address 3 is missing.
```

```
*Jun  7 22:58:01.509: %IOSXE-3-PLATFORM: R1/0: kernel: mdio_bus ffb4fc000: MDIO device at
address 4 is missing.
*Jul 26 08:29:51.405: %IOSXE_OIR-6-ONLINECARD: Card (rp) online in slot R1
*Jul 26 08:29:51.430: %IOSXE_RP_ALARM-6-INFO: cleared MAJOR module R1: Boot state
*Jul 26 08:30:01.032: %SYSHW-3-SYSHW_REG_READ: R0/0: emd: A register read operation has
failed for device: I2C_FAN_CTRL register: /sys/bus/i2c/devices/21-0020/temp1_input  error:
 Invalid argument
*Jul 26 08:30:02.253: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 1
*Jul 26 08:30:02.265: %IOSXE_OIR-6-OFFLINECARD: Card (cc) offline in slot 1
*Jul 26 08:30:09.134: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F1
*Jul 26 08:30:33.646: %IOSXE-3-PLATFORM: R1/0: kernel: pcieport 0000:01:00.0:
of_irq_parse_pci() failed with rc=-22
*Jul 26 08:31:37.600: %IOSXE-3-PLATFORM: R1/0: uea_mgr: QDR 0 is Ready
*Jul 26 08:31:58.698: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))

*Jul 26 08:31:58.698: %IOSXE_RP_ALARM-6-INFO: cleared MAJOR module R0: Secondary removed
*Jul 26 08:31:58.699: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Jul 26 08:32:01.578: %REDUNDANCY-3-IPC: IOS versions do not match.

*Jul 26 08:32:02.483: %HA_EM-6-LOG: Mandatory.uearp_stby_ios_mismatch_eem.tcl: AUTOMATIC
UPGRADE: CHASSIS IS NOT NCS. HENCE ABORTING AUTOMATIC UPGRADE
*Jul 26 08:32:23.494: %CMRP-6-FP_HA_STATUS: R1/0: cmand: F0 redundancy state is Active with
 ready Standby
*Jul 26 08:32:23.669: %CMRP-6-FP_HA_STATUS: R0/0: cmand: F0 redundancy state is Active with
 ready Standby
*Jul 26 08:32:56.373: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 1
*Jul 26 08:33:57.534: %ISSU-3-INCOMPATIBLE_PEER_UID: Setting image
(PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), version (16.12.1prd15) on peer uid (49) as incompatible
*Jul 26 08:33:57.534: Config Sync: Bulk-sync failure due to Servicing Incompatibility.
Please check full list of mismatched commands via:
  show redundancy config-sync failures mcl

*Jul 26 08:33:57.534: Config Sync: Starting lines from MCL file:
-line aux 0
 ! <submode> "line"
 stopbits 1
! </submode> "line"

*Jul 26 08:33:58.540: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)Finished
wait for Standby RP to reach terminal redundancy state

STAGE 3: Installing sipspa package on local RP
================================================
--- Starting install local lock acquisition on R0 ---
Finished install local lock acquisition on R0

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting file path checking ---

*Jul 26 08:34:03.729: %INSTALL-5-OPERATION_START_INFO: R0/0: provision: Started install
package bootflash:issu/*rsp3-sipspa*16.12.01prd15.SPA*.pkgFinished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr900rsp3-sipspa.16.12.01prd15.SPA.pkg
```

```
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatibility verification ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatibility verification

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed asr900rsp3-sipspa.16.11.01a.SPA.pkg
New files list:
  Added asr900rsp3-sipspa.16.12.01prd15.SPA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
  Replacing running software
  Replacing CLI software
  Restarting software
ISSU Sequence file found.
  Processing IM: 0/0
  ETA to Process Next IM: 160 seconds
  Processing IM: 0/1
  ETA to Process Next IM: 160 seconds
  Processing IM: 0/2
  ETA to Process Next IM: 160 seconds
```

```
  Processing IM: 0/3
  ETA to Process Next IM: 160 seconds
  Processing IM: 0/4
  ETA to Process Next IM: 160 seconds
  Processing IM: 0/5
  ETA to Process Next IM: 160 seconds
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.

*Jul 26 09:00:23.807: %INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: provision: Completed install
 package bootflash:issu/*rsp3-sipspa*16.12.01prd15.SPA*.pkgSTAGE 4: Installing software on
 active RP
================================================
--- Starting install local lock acquisition on R0 ---
Finished install local lock acquisition on R0

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting file path checking ---

*Jul 26 09:00:31.390: %INSTALL-5-OPERATION_START_INFO: R0/0: provision: Started install
package bootflash:issu/*rsp3-*16.12.01prd15.SPA*.pkgFinished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr900rsp3-espbase.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpaccess.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpbase.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpboot.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpcontrol.16.12.01prd15.SPA.pkg
  Found asr900rsp3-rpios-universalk9_npe.16.12.01prd15.SPA.pkg
  Found asr900rsp3-sipbase.16.12.01prd15.SPA.pkg
  Found asr900rsp3-sipspa.16.12.01prd15.SPA.pkg
Verifying image file locations
Inspecting image file types
    WARNING: In-service installation of IOSD package
    WARNING: requires software redundancy on target RP
    WARNING: or on-reboot parameter
    WARNING: Automatically setting the on-reboot flag
    WARNING: In-service installation of RP Base package
    WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
```

```
Finished candidate package set construction

--- Starting ISSU compatibility verification ---
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished ISSU compatibility verification

--- Starting list of software package changes ---
Old files list:
  Removed asr900rsp3-espbase.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpaccess.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpbase.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpboot.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpcontrol.16.11.01a.SPA.pkg
  Removed asr900rsp3-rpios-universalk9_npe.16.11.01a.SPA.pkg
  Removed asr900rsp3-sipbase.16.11.01a.SPA.pkg
New files list:
  Added asr900rsp3-espbase.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpaccess.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpbase.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpboot.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpcontrol.16.12.01prd15.SPA.pkg
  Added asr900rsp3-rpios-universalk9_npe.16.12.01prd15.SPA.pkg
  Added asr900rsp3-sipbase.16.12.01prd15.SPA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

SUCCESS: Software provisioned.  New software will load on reboot.

*Jul 26 09:07:55.045: %INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: provision: Completed install
 package bootflash:issu/*rsp3-*16.12.01prd15.SPA*.pkgSTAGE 5: Restarting active RP (switchover
 to stdby)
================================================
--- Starting active reload ---
Finished active reload

SUCCESS: node ISSU finished successfully.
Jul 26 09:08:04.327: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: process
exit with reload fru code
Jul 26 09:08:05.622: %PMAN-5-EXITACTION: R0/0: pvp: Process manage

BootPage Setting Done - Next DDR-init


System Bootstrap, Version 15.6(33r)S, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2018 by cisco Systems, Inc.

Compiled Sat 06-Oct-18 23:23 by pallavik

Starting Initialization of FMAN0

Loading ucode for FMAN0, size: 31424, ver: 106.04.14
```

```
fixup address:7ffff278 contentsoffixup:7ffff000
DCFG_CCSR_PORSR1(cfg_0_9 pins):22FB7F7F
RC Vendor ID[0x8241957]
PEX up stream Vendor ID[0x860910b5]
PEX down stream vendor ID [0x860910b5]
FPGA vendor ID[0x5f1137]
PCI Configuration done..
IOFPGA version[19052734]

Current image running: Boot ROM0
Last reset cause: RSP-Board
Configuring zarlink...
C-Inlet temp 40C
ARAD-0 temp 55C
UEA platform with 3670016 Kbytes of main memory

Checking eUSB devices..
USB PHY clock valid[0x20000]
USB0:   USB EHCI 1.00
allocating the qtd buffer..
scanning bus 0 for devices... port 1 connection change
hub_port_reset: resetting port 0...
STAT_C_CONNECTION = 0 STAT_CONNECTION = 1  USB_PORT_STAT_ENABLE 1
hub_port_reset: resetting port 0...
STAT_C_CONNECTION = 0 STAT_CONNECTION = 1  USB_PORT_STAT_ENABLE 1
port 1 connection change
hub_port_reset: resetting port 0...
STAT_C_CONNECTION = 0 STAT_CONNECTION = 1  USB_PORT_STAT_ENABLE 1
hub_port_reset: resetting port 0...
STAT_C_CONNECTION = 0 STAT_CONNECTION = 1  USB_PORT_STAT_ENABLE 1
3 USB Device(s) found
USB1:   USB EHCI 1.00
scanning bus 1 for devices... 1 USB Device(s) found
```

```
       scanning usb for storage devices... 1 Storage Device(s) found

Located issu/packages.conf

Image size 8034 inode num 32464, bks cnt 2 blk size 8*512

#

Located issu/asr900rsp3-rpboot.16.12.01prd15.SPA.pkg

Image size 35163995 inode num 32461, bks cnt 8585 blk size 8*512

############################################################################################################

Boot image size = 35163995 (0x2188f5b) bytes


Package header rev 3 structure detected

Calculating SHA-1 hash...done

validate_package_cs: SHA-1 hash:

 calculated 1910f63e:c01a63ee:18d0e6d1:ebf6233c:e445a270

 expected   1910f63e:c01a63ee:18d0e6d1:ebf6233c:e445a270


No suitable keys found in the key storage. 22

RSA Signed RELEASE Image Signature Verification Successful.

Image validated

Passing control to the main image..


              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [Gibraltar], ASR900 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version
 16.12.1prd15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Sat 20-Jul-19 12:25 by mcpre



PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
```

```
"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL
ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU
ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement
(EULA) and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are
licensed for a particular term, that the license to such Software and/or
features is valid only for the applicable term and that such Software and/or
features may be shut down or otherwise terminated by Cisco after expiration
of the applicable license term (e.g., 90-day trial period). Cisco reserves
the right to terminate any such Software feature electronically or by any
other means available. While Cisco may provide alerts, it is your sole
responsibility to monitor your usage of any such term Software feature to
ensure that your systems and networks are prepared for a shutdown of the
Software feature.



All TCP AO KDF Tests Pass
cisco ASR-903 (RSP3_200) processor (revision RSP3_200) with 1948285K/6147K bytes of memory.
Processor board ID FOX1606P060
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
5703875K bytes of eMMC flash at bootflash:.

Authentication passed
```



Note

```
scanning usb for storage devices... 1 Storage Device(s) found
```

In the above output, the USB and storage device denote the following:

- **“scanning usb for storage devices”**---> It is a print that indicates to check as a part of USB scanning.
- **1 Storage Device(s) found**---> This denotes the number of storage devices that are found. The default bootflash is a storage device, hence it shows as above.

The system always counts the internal bootflash as one storage device. So even without a USB, it shows as 1 device found. When a USB is connected and detected, the message updates to:

```
scanning usb for storage devices... 2 Storage Device(s) found
```

This indicates that:

- 1 device = bootflash
- 1 device = USB

Example: Single Command Software Upgrade

```
Router# request platform software package install node file bootflash:XE371_k9_0810.bin
interface-module-delay 150
```

```
NOTE: Currently node has booted from a provisioning file
NOTE: Going to start a dual rp sub-packages node ISSU install
--- Starting initial file path checking ---
Copying bootflash:XE371_k9_0810.bin to stby-bootflash:XE371_k9_0810.bin
Finished initial file path checking
--- Starting config-register verification ---
Finished config-register verfication
--- Starting image file expansion ---
Expanding image file: bootflash:XE371_k9_0810.bin
Image file expanded and copied
Expanding image file: stby-bootflash:XE371_k9_0810.bin
Image file expanded and copied
Finished image file expansion
STAGE 1: Installing software on standby RP
==========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Found asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Found asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
    WARNING: In-service installation of IOSD package
    WARNING: requires software redundancy on target RP
    WARNING: or on-reboot parameter
    WARNING: Automatically setting the on-reboot flag
    WARNING: In-service installation of RP Base package
    WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
Determining whether installation is valid
Determining whether installation is valid ... skipped
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
```

```
Checking package specific compatibility
Finished compatibility testing
--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-espbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpaccess.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpcontrol.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpios-universalk9_npe.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipspa.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Added asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.
STAGE 2: Restarting standby RP
==============================
--- Starting standby reload ---
Finished standby reload
--- Starting wait for Standby RP to reach terminal redundancy state ---
Finished wait for Standby RP to reach terminal redundancy state
STAGE 3: Installing sipspa package on local RP
==============================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
```

```
Determining whether installation is valid
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Software sets are identified as compatible
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished compatibility testing
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-sipspa.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
  Replacing running software
  Replacing CLI software
  Restarting software
  Restarting IM: 0/0
Skipping IM reload for Ethernet IM
  Restarting IM: 0/1
Skipping IM reload for Ethernet IM
  Restarting IM: 0/2
Skipping IM reload for Ethernet IM
  Restarting IM: 0/3
Skipping IM reload for Ethernet IM
  Restarting IM: 0/4
Skipping IM reload for Ethernet IM
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
STAGE 4: Installing software on active RP
========================================
```

```
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Found asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
    WARNING: In-service installation of IOSD package
    WARNING: requires software redundancy on target RP
    WARNING: or on-reboot parameter
    WARNING: Automatically setting the on-reboot flag
    WARNING: In-service installation of RP Base package
    WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
Determining whether installation is valid
Determining whether installation is valid ... skipped
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished compatibility testing
--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-espbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpaccess.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpcontrol.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpios-universalk9_npe.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipbase.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Added asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
```

```
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.
STAGE 5: Restarting active RP (switchover to stdby)
================================================
--- Starting active reload ---
Finished active reload
SUCCESS: node ISSU finished successfully.
RUDY-1#
RUDY-1#Aug 24 07:54:41.715 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: reload fru
 action requested
System Bootstrap, Version 15.3(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.
Compiled Tue 26-Jun-12 12:42 by ccai
Current image running: Boot ROM0UEA platform with 3670016 Kbytes of main memory
Located packages.conf
Image size 7519 inode num 38, bks cnt 2 blk size 8*512
#
Located asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Image size 34216240 inode num 90631, bks cnt 8354 blk size 8*512
###################################################################################
###################################################################################
###################################################################################
###################################################################################
Boot image size = 34216240 (0x20a1930) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
        calculated e7674970:dbc1eb86:325219c7:b3da0e0f:077e5e4d
        expected   e7674970:dbc1eb86:325219c7:b3da0e0f:077e5e4d
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): load_crash_kernel took: 2 seconds, expected
max time 2 seconds
%IOSXEBOOT-4-DEBUG_CONF: (rp/0): File /bootflash/debug.conf is absent, ignoring
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): Chassis initialization took: 26 seconds,
expected max time 10 seconds
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): upgrade hw-programmable took: 2 seconds,
expected max time 2 seconds
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M),
Experimental Version 15.2(20120810:081250)
[v152_4_s_xe37_throttle-BLD-BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021-ios 131]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 10-Aug-12 03:50 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
```

```
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ASR-903 (RSP1) processor with 540359K/6147K bytes of memory.
Processor board ID FOX1518P0GP
32768K bytes of non-volatile configuration memory.
3670016K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.
Press RETURN to get started!
```



Note

```
scanning usb for storage devices... 1 Storage Device(s) found
```

In the above output, the USB and storage device denote the following:

- **“scanning usb for storage devices”**---> It is a print that indicates to check as a part of USB scanning.
- **1 Storage Device(s) found**---> This denotes the number of storage devices that are found. The default bootflash is a storage device, hence it shows as above.

The system always counts the internal bootflash as one storage device. So even without a USB, it shows as 1 device found. When a USB is connected and detected, the message updates to:

```
scanning usb for storage devices... 2 Storage Device(s) found
```

This indicates that:

- 1 device = bootflash
- 1 device = USB

Fast Booting the RSP3 .bin Image

Table 12: Feature History

Feature Name	Release Information	Feature Description
Fast Booting the RSP3 .bin Image	Cisco IOS XE Amsterdam 17.3.1	A new command **platform fastboot** is introduced on the RSP3 module. When enabled on the RSP3 module that is pre-booted with .bin image, on the next reboot, the ROMMON boots up with the corresponding packages.conf image. Boot up from the packages.conf image is much faster and thus, the boot time is reduced approximately by six to eight minutes.

Effective with Cisco IOS XE Release 17.3.1, **platform fastboot** command is introduced on the RSP3 module. When enabled on the RSP3 module that is pre-booted with .bin image, on the next reboot, the ROMMON boots up with the corresponding packages.conf image. Boot up from the packages.conf image is much faster and thus, the boot time is reduced approximately by six to eight minutes.

Limitations

- ISSU is not supported.
- ROMMON version 15.6(36r)S or above must be present.
- If the autoboot image name is changed when the **platform fastboot** command is already enabled, the **platform fastboot** command gets disabled.

The following procedure explains how to enable the **platform fastboot** command.

```
Router#enable
Router#configure terminal
Router(conf)#platform fastboot
Router(conf)#end
```

Use the following command to verify that the **platform fastboot** command is enabled.

```
Router#show running-config | i fastboot
platform fastboot
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS master command list	Cisco IOS Master Command List , All Releases

Related Topic	Document Title
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

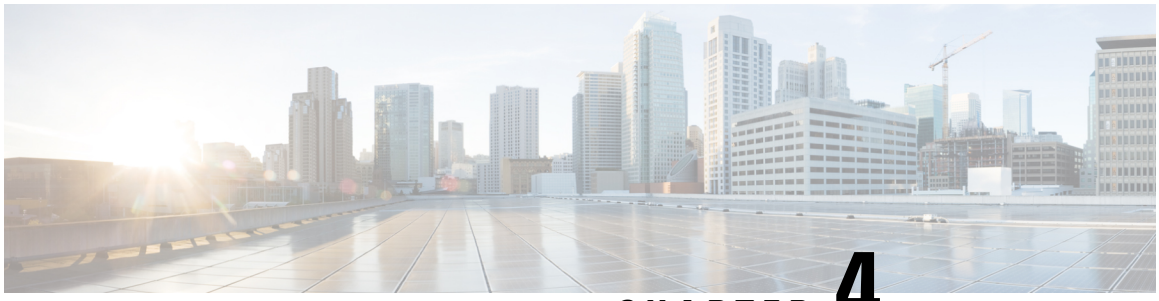
MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified. Cisco ASR 900 Series Aggregation Services Routers MIB Specifications Guide	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs Cisco ASR 900 Series Aggregation Services Routers MIB Specifications Guide

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 4

Configuring Stateful Switchover

The Stateful Switchover (SSO) feature works with Nonstop Forwarding (NSF) in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The primary objective of SSO is to improve the availability of networks constructed with Cisco routers. SSO performs the following functions:

- Maintains stateful protocol and application information to retain user session information during a switchover.
- Enables line cards to continue to forward network traffic with no loss of sessions, providing improved network availability.
- Provides a faster switchover relative to high system availability.

- Prerequisites for Stateful Switchover, on page 53
- Restrictions for Stateful Switchover, on page 54
- Information About Stateful Switchover, on page 55
- Enhanced SNMP Support for High Availability, on page 64
- How to Configure Stateful Switchover, on page 67
- Configuration Examples for Stateful Switchover, on page 73

Prerequisites for Stateful Switchover

General Prerequisites

- Both RSPs must be running the same version of Cisco software.
- Before copying a file to flash memory, be sure that ample space is available in flash memory. Compare the size of the file you are copying to the amount of available flash memory shown. If the space available is less than the space required by the file you will copy, the copy process will not continue and an error message similar to the following will be displayed:

```
%Error copying tftp://image@server/tftpboot/filelocation/imagename (Not enough space on
device).
```

-

- For Nonstop Forwarding (NSF) support, neighbor routers must be running NSF-enabled images, though SSO need not be configured on the neighbor device.

SNMP for Stateful Switchover Prerequisites

SNMP must be configured. See the Configuring SNMP Support module of Cisco IOS XE Network Management Configuration Guide for configuration information. There are no configuration tasks for SNMP for SSO.

Restrictions for Stateful Switchover

General Restrictions for SSO

- Only SSO mode is supported.
- Configuration changes made through SNMP may not be automatically configured on the standby RP after a switchover occurs.
- Enhanced Object Tracking (EOT) is not stateful switchover-aware and cannot be used with HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) in SSO mode.

Configuration Mode Restrictions

- The configuration registers on both RPs must be set the same for the networking device to behave the same when either RP is rebooted.
- During the startup (bulk) synchronization, configuration changes are not allowed. Before making any configuration changes, wait for a message similar to the following:

```
%HA-5-MODE:Operating mode is sso, configured mode is sso.
HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
```

Switchover Process Restrictions

- If the router is configured for SSO mode, and the active RP fails before the standby is ready to switch over, the router will recover through a full system reset.

Cisco ASR 903 Series Aggregation Services Routers Restrictions

- Only SSO mode is supported on Cisco ASR 903 Aggregation Services routers.
- All licenses are synced to the standby RSP, when evaluation or permanent licenses are installed on a HA system. However, when a new RSP is inserted in a standby system for HA, the standby RSP resets once before it reaches standby hot state.
- Erasing router configuration using **write erase** command does not work in standby router in HA system when it is applied from an active router or when accessed from telnet.

SNMP for Stateful Switchover Restrictions

- Statistics and counter values will not be synchronized from the active to the standby RP.
- Only the MIBs listed in the SSO MIB Support section are synchronized between the active and the standby RPs.
- SNMP requests can fail during the switchover process, that is, while the standby RP is taking over as the active RP. Data in the unsynchronized MIBs may be out of synchronization, and the information in these MIBs can be lost on a switchover.
- Synchronization of SNMP data between RPs is available only when the networking device is operating in SSO mode.

Information About Stateful Switchover

SSO Overview

SSO provides protection for network edge devices with dual RPs that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

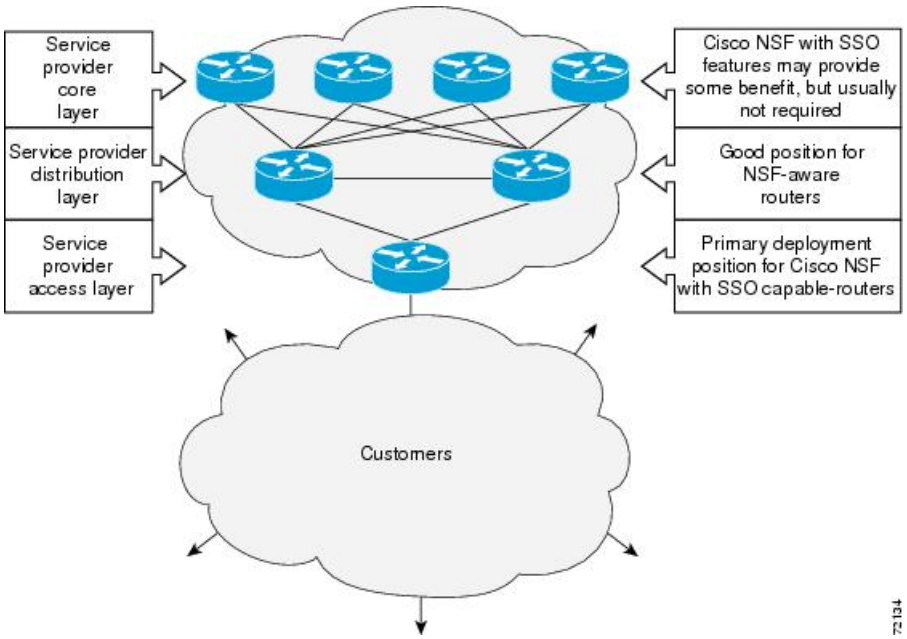
In Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

SSO is used with the Cisco Nonstop Forwarding (NSF) feature. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps, thereby reducing loss of service outages for customers.

The figure below illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is primarily at the access layer (edge) of the service provider network. A fault at this point could result in loss of service for enterprise customers requiring access to the service provider network.

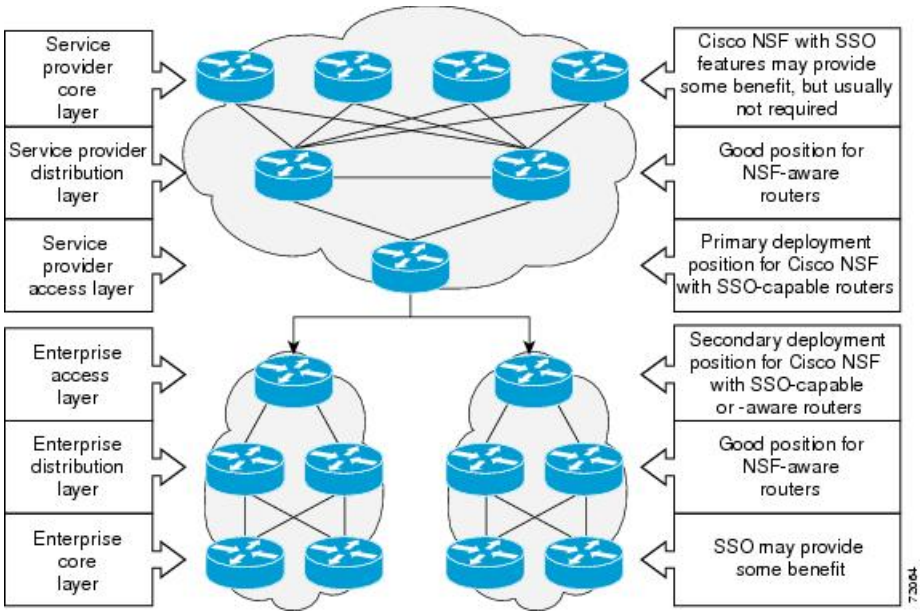
Figure 1: Cisco NSF with SSO Network Deployment: Service Provider Networks



For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Additional network availability benefits might be achieved by applying Cisco NSF and SSO features at the core layer of your network; however, consult your network design engineers to evaluate your specific site requirements.

Additional levels of availability may be gained by deploying Cisco NSF with SSO at other points in the network where a single point of failure exists. The figure below illustrates an optional deployment strategy that applies Cisco NSF with SSO at the enterprise network access layer. In this example, each access point in the enterprise network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

Figure 2: Cisco NSF with SSO Network Deployment: Enterprise Networks



Redundancy Modes

Stateful Switchover Mode

SSO supports synchronization of line card, protocol, and application state information between RPs for supported features and protocols (a hot standby).

Route Processor Synchronization

In networking devices running SSO, both RPs must be running the same configuration so that the standby RP is always ready to assume control if the active RP fails.

To achieve the benefits of SSO, synchronize the configuration information from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. This synchronization occurs in two separate phases:

- While the standby RP is booting, the configuration information is synchronized in bulk from the active RP to the standby RP.
- When configuration or state changes occur, an incremental synchronization is conducted from the active RP to the standby RP.

Note Effective Cisco IOS XE Amsterdam 17.2.1, standby inventory files are automatically created during the bootup of the standby RSP. This process reduces the time taken to send the RF notification to the client protocol by **one** second.

Bulk Synchronization During Initialization

When a system with SSO is initialized, the active RP performs a chassis discovery (discovery of the number and type of line cards and fabric cards, if available, in the system) and parses the startup configuration file.

The active RP then synchronizes this data to the standby RP and instructs the standby RP to complete its initialization. This method ensures that both RPs contain the same configuration information.

Even though the standby RP is fully initialized, it interacts only with the active RP to receive incremental changes to the configuration files as they occur. Executing CLI commands on the standby RP is not supported.

During system startup, the startup configuration file is copied from the active RP to the standby RP. Any existing startup configuration file on the standby RP is overwritten. The startup configuration is a text file stored in the NVRAM of the RP. It is synchronized whenever you perform the following operations:

- The command **copy system:running-config nvram:startup-config** is used.
- The command **copy running-config startup-config** is used.
- The command **write memory** is used.
- The command **copy** *filename* **nvram:startup-config** is used.
- SNMP SET of MIB variable ccCopyEntry in CISCO_CONFIG_COPY MIB is used.
- System configuration is saved using the **reload** command.
- System configuration is saved following entry of a forced switchover command.

Incremental Synchronization

After both RPs are fully initialized, any further changes to the running configuration or active RP states are synchronized to the standby RP as they occur. Active RP states are updated as a result of processing protocol information, external events (such as the interface becoming up or down), or user configuration commands (using Cisco IOS commands or Simple Network Management Protocol [SNMP]) or other internal events.

Changes to the running configuration are synchronized from the active RP to the standby RP. In effect, the command is run on both the active and the standby RP.

Configuration changes caused by an SNMP set operation are synchronized on a case-by-case basis. Only two SNMP configuration set operations are supported:

- **shut** and **no-shut** (of an interface)
- **link up/down trap** *enable/disable*

Routing and forwarding information is synchronized to the standby RP:

- State changes for SSO-aware protocols (ATM, Frame Relay, PPP, High-Level Data Link Control [HDLC]) or applications (SNMP) are synchronized to the standby RP.
- Cisco Express Forwarding (CEF) updates to the Forwarding Information Base (FIB) are synchronized to the standby RP.

Chassis state changes are synchronized to the standby RP. Changes to the chassis state due to line card insertion or removal are synchronized to the standby RP.

Changes to the line card states are synchronized to the standby RP. Line card state information is initially obtained during bulk synchronization of the standby RP. Following bulk synchronization, line card events,

such as whether the interface is up or down, received at the active processor are synchronized to the standby RP.

The various counters and statistics maintained in the active RP are not synchronized because they may change often and because the degree of synchronization they require is substantial. The volume of information associated with statistics makes synchronizing them impractical.

Not synchronizing counters and statistics between RPs may create problems for external network management systems that monitor this information.

Switchover Operation

Switchover Conditions

An automatic or manual switchover may occur under the following conditions:

- A fault condition that causes the active RP to crash or reboot--automatic switchover
- The active RP is declared dead (not responding)--automatic switchover
- The command is invoked--manual switchover

The user can force the switchover from the active RP to the standby RP by using a CLI command. This manual procedure allows for a graceful or controlled shutdown of the active RP and switchover to the standby RP. This graceful shutdown allows critical cleanup to occur.

Note This procedure should not be confused with the graceful shutdown procedure for routing protocols in core routers--they are separate mechanisms.

Caution The SSO feature introduces a number of new command and command changes, including commands to manually cause a switchover. The **reload** command does not cause a switchover. The **reload** command causes a full reload of the box, removing all table entries, resetting all line cards, and interrupting nonstop forwarding.

Switchover Time

Switchover time is only a few seconds on the router. Packets that are switched or routed by the ASIC are not impacted by the RP switchover. However, if packets are punted to the RP for further processing, switching and routing will be impacted. The length of time can be due to a number of factors including the time needed for the previously active processor to obtain crash information, load code and microcode, and synchronize configurations between processors and line protocols and Cisco NSF-supported protocols.

Core Dump Operation

In networking devices that support SSO, the newly active primary processor runs the core dump operation after the switchover has taken place. Not having to wait for dump operations effectively decreases the switchover time between processors.

Following the switchover, the newly active RP will wait for a period of time for the core dump to complete before attempting to reload the formerly active RP. The time period is configurable. For example, on some

platforms an hour or more may be required for the formerly active RP to perform a coredump, and it might not be site policy to wait that much time before resetting and reloading the formerly active RP. In the event that the core dump does not complete within the time period provided, the standby is reset and reloaded regardless of whether it is still performing a core dump.

The core dump process adds the slot number to the core dump file to identify which processor generated the file content.

Note Core dumps are generally useful only to your technical support representative. The core dump file, which is a very large binary file, must be transferred using the TFTP, FTP, or remote copy protocol (rcp) server and subsequently interpreted by a Cisco Technical Assistance Center (TAC) representative that has access to source code and detailed memory maps.

SSO-Aware Protocols and Applications

SSO-supported line protocols and applications must be SSO-aware. A feature or protocol is SSO-aware if it maintains, either partially or completely, undisturbed operation through an RP switchover. State information for SSO-aware protocols and applications is synchronized from active to standby to achieve stateful switchover for those protocols and applications.

The dynamically created state of SSO-unaware protocols and applications is lost on switchover and must be reinitialized and restarted on switchover.

SSO-aware applications are either platform-independent, such as in the case of line protocols or platform-dependent (such as line card drivers). Enhancements to the routing protocols (Cisco Express Forwarding, Open Shortest Path First, and Border Gateway Protocol [BGP]) have been made in the SSO feature to prevent loss of peer adjacency through a switchover; these enhancements are platform-independent.

Line Protocols

SSO-aware line protocols synchronize session state information between the active and standby RPs to keep session information current for a particular interface. In the event of a switchover, session information need not be renegotiated with the peer. During a switchover, SSO-aware protocols also check the line card state to learn if it matches the session state information. SSO-aware protocols use the line card interface to exchange messages with network peers in an effort to maintain network connectivity.

ATM Stateful Switchover

With stateful switchover, ATM dynamic state information is synchronized between the active RP and standby RP. Thus when the active RP fails, the standby RP can take over without spending excessive time relearning the dynamic state information, and forwarding devices can continue to forward packets with only a few seconds of interruption (less on some platforms).

Note ATM SSO is not configurable and runs by default on networking devices configured with ATM and Redundancy Mode SSO.

Note ATM SSO is *not* supported on the ASR 900 RSP3 Module in Cisco IOS Release 3.16.

Permanent Virtual Circuits

For ATM to support forwarding during and after switchover, ATM permanent virtual circuits (PVCs) must remain up not only within the networking device, but also within the ATM network.

In an ATM network, all traffic to or from an ATM interface is prefaced with a virtual path identifier (VPI) and virtual channel identifier (VCI). A VPI-VCI pair is considered a single virtual circuit. Each virtual circuit is a private connection to another node on the ATM network. In ATM SSO, the VPI-VCI pair is associated with a virtual circuit descriptor (VCD). ATM SSO uses VCD information in synchronizing VPI-VCI information to the standby RP.

Each virtual circuit is treated as a point-to-point or point-to-multipoint mechanism to another networking device or host and can support bidirectional traffic. On point-to-point subinterfaces, or when static mappings are configured, Inverse Address Resolution Protocol (ARP) need not run. In cases where dynamic address mapping is used, an Inverse ARP protocol exchange determines the protocol address to VPI-VCI mapping for the PVC. This process occurs as soon as the PVC on a multipoint subinterface makes the transition to active. If that process fails for some reason, the remote networking device may drop the Inverse ARP request if it has not yet seen the PVC transition to active. Inverse ARP runs every 60 seconds to relearn the dynamic address mapping information for the active RP.

Note Permanent Virtual Circuits are *not* supported on the ASR 900 RSP3 Module in Cisco IOS Release 3.16.

PPP and Multilink PPP Stateful Switchover

With stateful switchover, specific PPP state information is synchronized between the active RP and standby RP. Thus when the active RP fails, the standby RP can take over without spending excessive time renegotiating the setup of a given link. As long as the physical link remains up, forwarding devices can continue to forward packets with only a few seconds of interruption (less on some platforms). Single-link PPP and Multilink PPP (MLP) sessions are maintained during RP switchover for IP connections only.

PPP and MLP support many Layer 3 protocols such as IPX and IP. Only IP links are supported in SSO. Links supporting non IP traffic will momentarily renegotiate and resume forwarding following a switchover. IP links will forward IP traffic without renegotiation.

A key factor in maintaining PPP session integrity during a switchover is the use of keepalive messages. This keepalive mechanism provides an exchange of information between peer interfaces to verify data and link integrity. Depending on the platform and configuration, the time required for switchover to the standby RP might exceed the keepalive timeout period. PPP keepalive messages are started when the physical link is first brought up. By default, keepalive messages are sent at 10-second intervals from one PPP interface to the other PPP peer.

If five consecutive keepalive replies are not received, the PPP link would be taken down on the newly active RP. Caution should be used when changing the keepalive interval duration to any value less than the default setting.

Only in extremely rare circumstances could the RP switchover time exceed the default 50-second keepalive duration. In the unlikely event this time is exceeded, the PPP links would renegotiate with the peers and resume IP traffic forwarding.

Note PPP and MLP are not configurable and run by default on networking devices configured with SSO.

Note PPP and MLP are *not* supported on the ASR 900 RSP3 Module in Cisco IOS XE Release 3.16.

HDLC Stateful Switchover

With stateful switchover, High-Level Data Link Control (HDLC) synchronizes the line protocol state information. Additionally, the periodic timer is restarted for interfaces that use keepalive messages to verify link integrity. Link state information is synchronized between the active RP and standby RP. The line protocols that were up before the switchover remain up afterward as long as the physical interface remains up. Line protocols that were down remain down.

A key factor in maintaining HDLC link integrity during a switchover is the use of keepalive messages. This keepalive mechanism provides an exchange of information between peer interfaces to verify data is flowing. HDLC keepalive messages are started when the physical link is first brought up. By default, keepalive messages are sent at 10-second intervals from one HDLC interface to the other.

HDLC waits at least three keepalive intervals without receiving keepalive messages, sequence number errors, or a combination of both before it declares a line protocol down. If the line protocol is down, SSO cannot support continuous forwarding of user session information in the event of a switchover.

Note HDLC is not configurable and runs by default on networking devices configured with SSO.

Note HDLC is *not* supported on the A900 RSP3 Module in Cisco IOS XE Release 3.16.

Quality of Service

The modular QoS CLI (MQS)-based QoS feature maintains a database of various objects created by the user, such as those used to specify traffic classes, actions for those classes in traffic policies, and attachments of those policies to different traffic points such as interfaces. With SSO, QoS synchronizes that database between the primary and secondary RP.

IPv6 Support for Stateful Switchover

IPv6 neighbor discovery supports SSO using Cisco Express Forwarding. When switchover occurs, the Cisco Express Forwarding adjacency state, which is checkpointed, is used to reconstruct the neighbor discovery cache.

Line Card Drivers

Platform-specific line card device drivers are bundled with the Cisco software image for SSO and are correct for a specific image, meaning they are designed to be SSO-aware.

Line cards used with the SSO feature periodically generate status events that are forwarded to the active RP. Information includes the line up or down status, and the alarm status. This information helps SSO support bulk synchronization after standby RP initialization and support state reconciliation and verification after a switchover.

Line cards used with the SSO feature also have the following requirements:

- Line cards must not reset during switchover.
- Line cards must not be reconfigured.
- Subscriber sessions may not be lost.



Note The standby RP communicates only with the active RP, never with the line cards. This function helps to ensure that the active and standby RP always have the same information.

Routing Protocols and Nonstop Forwarding

Cisco nonstop forwarding (NSF) works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. When a networking device restarts, all routing peers of that device usually detect that the device went down and then came back up. This down-to-up transition results in what is called a "routing flap," which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Cisco NSF helps to suppress routing flaps, thus improving network stability.

Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards to remain up through a switchover and to be kept current with the FIB on the active RP is key to Cisco NSF operation.

A key element of Cisco NSF is packet forwarding. In Cisco networking devices, packet forwarding is provided by Cisco Express Forwarding. Cisco Express Forwarding maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature eliminates downtime during the switchover.

Cisco NSF supports the BGP, IS-IS, and OSPF routing protocols. In general, these routing protocols must be SSO-aware to detect a switchover and recover state information (converge) from peer devices. Each protocol depends on Cisco Express Forwarding to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables.

Network Management

Network management support for SSO is provided through the synchronization of specific SNMP data between the active and standby RPs. From a network management perspective, this functionality helps to provide an uninterrupted management interface to the network administrator.



Note Synchronization of SNMP data between RPs is available only when the networking device is operating in SSO mode.

Enhanced SNMP Support for High Availability

SNMP for Stateful Switchover Overview

The SNMP and stateful switchover feature helps to improve the availability of networks made up of Cisco networking devices. Using SSO, a networking device with redundant RPs will continue forwarding traffic, continue operating as a routing protocol peer, and remain manageable under a set of circumstances that ordinarily would cause an interruption in service.

The SSO feature allows one of the processors on the networking device to operate as the active RP, which passes the necessary system, routing, and application state information to the standby RP. Upon switchover, the standby RP quickly assumes the role of active RP. The goal of SNMP network management with SSO functionality is to provide an uninterrupted management interface to the end user during and after a switchover.

SNMP network management with SSO functionality ensures an uninterrupted management interface to the end user. The network administrator can differentiate a switchover from a system restart based on the notification type (for example, ciscoRFSwactNotif for switchover and coldStart or warmStart for system restarts). Uninterrupted service also includes synchronizing the SNMP configuration and data from core MIBs such as IF-MIB and ENTITY-MIB to the standby RP.

Network Management for SSO

Table 13: Feature History

Feature Name	Release Information	Description
Monitoring alarms for standby RSP management interface	Cisco IOS XE 17.15.1b	In addition to Active RSP, alarms are now generated for the management interface of the Stand-by RSP. You can monitor these alarms in Cisco's EPNM (Evolved Programmable Network Manager) and take the appropriate action to fix the problem.

Network management support for SSO is provided through the synchronization of specific SNMP data between the active and standby RPs. From a network management perspective, this synchronization helps to provide an uninterrupted management interface to the network administrator.

Synchronization of SNMP data between RPs is available only when the networking device is operating in SSO mode.

Uninterrupted Service Using SSO

When a networking device uses SSO, the network management engine of the standby RP should be indistinguishable from the network management engine of the active RP. A network management system (NMS) should not interpret a switchover to mean that a new device has come up.

The sysUpTime MIB object reports the system uptime. To prevent a switchover from being flagged as a restart, this object is synchronized between the active and the standby RPs. As a result, no coldStart or warmStart traps will be generated as a result of the switchover--the ciscoRFSwactNotif notification is used to signal a switchover.

Communication with the NMS

Counters and Statistics

The various counters and statistics maintained in the RP are not synchronized because they may change often and the degree of synchronization they require is substantial. They also are not critical to the system operation. Because of this lack of synchronization, counter objects experience a discontinuity after a switchover. The cRFStatusFailoverTime will be the value of sysUpTime when any one or more of the counters experiences a discontinuity.

Switchover Notification

The ciscoRFSwactNotif notification informs the NMS about a switchover. This notification provides information regarding the unit ID of the originator of the notification, the newly active redundant unit, the sysUptime data, and reason codes for why a switchover has occurred. The NMS can then use the ciscoRFSwactNotif notification to resynchronize the counter statistics values, if necessary.

Traps

Only notifications generated on the active RP are sent to the notification destination. None of the notifications generated on the standby RP are sent to the notification destination. Furthermore, notifications can be lost if they were generated on the active RP before a switchover. The NMS should be aware of these constraints.

SSO MIB Support

The CISCO-RF-MIB provides configuration control and status for the redundancy facility (RF) subsystem.

MIBs that are not listed in this section do not synchronize data between the redundant units. MIB synchronization for SSO only occurs when the system is in SSO mode.

All the objects in the following MIBs that contain SNMP configuration data are synchronized between the active and standby RPs:

- SNMP-FRAMEWORK-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMP-VACM-MIB
- SNMPv2-MIB

The following core MIBs support SSO:

- ENTITY-MIB—After a switchover, there will be no change in the data reported by the ENTITY-MIB object. This lack of change is result of the entPhysicalIndex and its associated objects being synchronized between the active and the standby RPs. The associated objects of the entPhysicalIndex are as follows:
  - entPhysicalAlias
  - entPhysicalSerialNum
  - entPhysicalAssetID
  - entLastChangeTime

- IF-MIB—The ifIndex is synchronized between the active and standby RPs, along with the ifNumber, ifTableLastChange, ifAdminStatus, ifLinkUpDownTrapEnable, ifAlias, ifLastChange, and ifStackLastChange objects.

The following infrastructure MIBs support SSO:

- Community MIB
- Notification MIB
- Notification log MIB
- Field-replaceable unit (FRU) control MIB
- CISCO-ENHANCED-MEMPOOL-MIB

CISCO-RF-MIB Modifications for SSO Support

New cRFHistorySwitchOverTable Table in CISCO-RF-MIB for SSO Support

The cRFHistorySwitchOverTable tracks the history of switchovers that have occurred since system initialization. New objects that have been added as part of this table are as follows:

- cRFHistoryPrevActiveUnitId--A read-only object that indicates the active RP that went down. The value of this object is the unique ID of the active RP that has gone down. The ID can be the slot ID, the physical or logical entity ID, or a unique ID assigned by the RF.
- cRFHistoryCurrActiveUnitId--A read-only object that indicates the standby RP that took over as the active RP. The value of this object is the unique ID of the active RP. The ID can be the slot ID, the physical or logical entity ID, or a unique ID assigned by the RF.
- cRFHistorySwitchOverReason--A read-only object that indicates the reason for the switchover. The reasons for the switchover from the active RP to the standby RP can be any of the following:
  - unsupported—This feature is unsupported.
  - none—No switchover has occurred.
  - notKnown—The reason is unknown.
  - userInitiated—A safe, manual switchover was initiated by the user.
  - userForced—A manual switchover was forced by the user. Preconditions, warnings, and safety
  - checks were ignored.
  - activeUnitFailed—An active RP fault caused an automatic switchover.
  - activeUnitRemoved—The active RP was removed, which caused an automatic switchover.
  - cRFHistorySwactTime—A read-only object that indicates the date and time the switchover occurred. The value of this object is a time stamp with the date and time the switchover occurred.

New Objects in CISCO-RF-MIB for SSO Support

The object added to the new cRFHistory subgroup are as follows:

- cRFHistoryTableMaxLength--A read-write object that indicates the maximum number of entries permissible in the history table. The value of this object is an integer that is more than 0. A value of 0 results in no history being maintained.
- cRFHistoryColdStarts--A read-only object that indicates the number of system cold starts including the number of system cold starts due to switchover fault and the number of manual restarts.
- cRFHistoryStandByAvailTime--A read-only object that indicates the cumulative time that a standby redundant unit has been available since the last system initialization.

  Two objects related to switchover status have also been added:

- cRFStatusFailoverTime--A read-only object that indicates the sysUpTime value when the primary redundant unit took over as active. The value of this object is 0 until the first switchover.
- cRFStatusPeerStandByEntryTime--A read-only object that indicates the sysUpTime value when the peer redundant unit entered the standbyHot state. The value of this object is 0 on system initialization.

How to Configure Stateful Switchover

Copying an Image onto an RP

To copy an image onto the active and standby RPs, follow these steps:

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **copy tftp bootflash:***filename*

Example:

```
Router# copy tftp bootflash:image1.bin
```

Copies a Cisco software image onto the flash device of the active RP.

Step 3 **copy tftp stby-bootflash:** *filename*

Example:

```
Router# copy tftp stby-bootflash:image1.bin
```

Copies a Cisco software image onto the flash device of the standby RP.

Step 4 **exit**

Example:

```
Router# exit
```

Exits to user EXEC mode.

Setting the Configuration Register and Boot Variables

To set the configuration register value and boot variables, follow these steps:

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show version**

Example:

```
Router# show version
```

Obtains the current configuration register setting.

Step 3 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 4 **no boot system** {**flash** [*filename*] | **tftp** *filename* [*ip-address*]}

Example:

```
Router(config)# no boot system flash
```

(Optional) Clears any existing system flash or TFTP boot image specification.

Step 5 **boot system** {**flash** [*filename*] | **tftp** *filename* [*ip-address*]}

Example:

```
Router(config)# boot system flash
```

Specifies the filename of stored image in flash memory or on a TFTP server.

Step 6 **config-register** *value*

Example:

```
Router(config)# config-register 0x2102
```

Modifies the existing configuration register setting to reflect the way in which you want to load a system image.

Step 7 **exit**

Example:

```
Router(config)# exit
```

Exits global configuration mode and returns the router to privileged EXEC mode.

Step 8 **copy running-config startup-config**

Example:

```
Router# copy running-config startup-config
```

Saves the configuration changes to the startup configuration file.

Step 9 **reload**

Example:

```
Router# reload
```

Reboots both RPs on the device to ensure that changes to the configuration take effect.

Configuring SSO

Before you begin

Image to be used by active or standby RP at initialization must be available on the local flash device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**mode sso** **Example:** `Router(config)# mode sso`	Sets the redundancy configuration mode to SSO on both the active and standby RP. **Note** After configuring SSO mode, the standby RP will automatically reset.
Step 5	**end** **Example:** `Router(config-red)# end`	Exits redundancy configuration mode and returns the router to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the configuration changes to the startup configuration file.

Verifying SSO Configuration

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show redundancy** [**clients** | **counters** | **history** | **switchover history** | **states**] **Example:** `Router# show redundancy`	Displays SSO configuration information.
Step 3	**show redundancy states** **Example:** `Router# show redundancy states`	Verifies that the device is running in SSO mode.

Troubleshooting Stateful Switchover

- The standby RP was reset, but there are no messages describing what happened--To display a log of SSO events and clues as to why a switchover or other event occurred, enter the **show redundancy history** command on the newly active RP.
- The show redundancy states command shows an operating mode that is different than what is configured on the networking device--On certain platforms the output of the **show redundancy states** command displays the actual operating redundancy mode running on the device, and not the configured mode as set by the platform. The operating mode of the system can change depending on system events. For example, SSO requires that both RPs on the networking device be running the same software image; if the images are different, the device will not operate in SSO mode, regardless of its configuration.
- Reloading the device disrupts SSO operation--The SSO feature introduces a number of commands, including commands to manually cause a switchover. The reload command is not an SSO command. This command causes a full reload of the box, removing all table entries, resetting all line cards, and thereby interrupting network traffic forwarding. To avoid reloading the box unintentionally, use the **redundancy force-switchover** command.
- During a software upgrade, the networking device appears to be in a mode other than SSO--During the software upgrade process, the show redundancy command indicates that the device is running in a mode other than SSO.

  This is normal behavior. Until the FSU procedure is complete, each RP will be running a different software version.
- You can enter ROM monitor mode by restarting the router and then pressing the Break key or issuing a **send break** command from a telnet session during the first 60 seconds of startup.The send break function can be useful for experienced users or for users under the direction of a Cisco Technical Assistance Center (TAC) representative to recover from certain system problems or to evaluate the cause of system problems.

Troubleshooting SSO

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**crashdump-timeout** [*mm* | *hh* **:** *mm*] **Example:** `router(config-red)# crashdump-timeout`	Set the longest time that the newly active RP will wait before reloading the formerly active RP.
Step 3	**debug atm ha-error** **Example:**	Debugs ATM HA errors on the networking device.

	Command or Action	Purpose
	`Router# debug atm ha-error`	
Step 4	**debug atm ha-events** **Example:** `Router# debug atm ha-events`	Debugs ATM HA events on the networking device.
Step 5	**debug atm ha-state** **Example:** `Router# debug atm ha-state`	Debugs ATM high-availability state information on the networking device.
Step 6	**debug ppp redundancy** [**detailed** | **event**] **Example:** `Router# debug ppp redundancy`	Debugs PPP redundancy on the networking device.
Step 7	**debug redundancy** {**all** | **ui** | **clk** | **hub**} **Example:** `Router# debug redundancy all`	Debugs redundancy on the networking device.
Step 8	**show diag** [*slot-number* | **chassis** | **subslot** *slot* / *subslot*] [**details** | **summary**] **Example:** `Router# show diag`	Displays hardware information for the router.
Step 9	**show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **switchover history** | **states** | **inter-device**] **Example:** `Router# show redundancy`	Displays the redundancy configuration mode of the RP. Also displays information about the number of switchovers, system uptime, processor uptime, and redundancy state, and reasons for any switchovers.
Step 10	**show version** **Example:** `Router# show version`	Displays image information for each RP.

Troubleshooting SNMP for Stateful Switchover

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**show redundancy history** **Example:** `Router# show redundancy history`	Displays switchover history.
Step 3	**show redundancy switchover history** **Example:** `Router# show redundancy switchover history`	Displays switchover history details.
Step 4	**debug snmp sync** **Example:** `Router# debug snmp sync`	Displays information about SNMP synchronization and faults in synchronization.
Step 5	**exir** **Example:** `Router# exit`	Exits to user EXEC mode.

Configuration Examples for Stateful Switchover

Example Configuring SSO

```
Router> enable
Router# configure terminal
Router(config)# redundancy
Router(config)# mode sso
Router(config-red)# end
Router# copy running-config startup-config
```

Example Verifying that SSO is Configured

In the following example, the **show redundancy** command is used to verify that SSO is configured on the device.

```
Router#show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 6 days, 4 hours, 17 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
```

```
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 4 hours, 16 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software (PPC_LINUX_
IOSD-UNIVERSALK9_NPE-M), Version 15.2(4)S3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 19-Apr-13 11:49 by mcpre
                        BOOT = bootflash:asr903rsp1-universalk9_npe.03.09.00.S
.153-2.S.bin,1;
        Configuration register = 0x2

Peer Processor Information :
----------------------------
              Standby Location = slot 7
        Current Software state = STANDBY HOT
       Uptime in current state = 6 days, 4 hours, 11 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software (PPC_LINUX_
IOSD-UNIVERSALK9_NPE-M), Version 15.2(4)S3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Mon 19-Apr-13 14:22 by mcpre
                        BOOT = bootflash:asr903rsp1-universalk9_npe.03.09.00.S
.153-2.S.bin,1;
                  CONFIG_FILE =
        Configuration register = 0x2
```

Example Verifying Redundancy-Related States

This is sample output of the **show redundancy states** command to verify the redundancy states.

```
Router#show redundancy states

       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 48

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 96
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

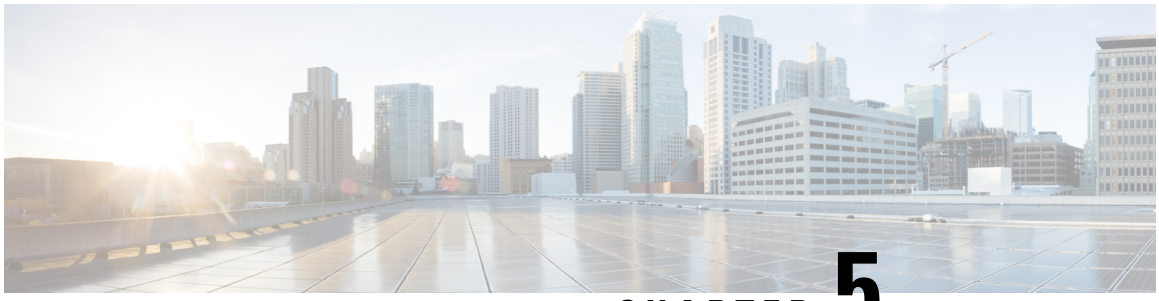
Example Verifying Redundancy-Aware Protocols and Applications

Enter the **show redundancy client** command to display the redundancy-aware applications and protocols.

```
Router# show redundancy client
clientID = 29 group_id = 1 clientSeq = 60 Redundancy Mode RF
```

```
clientID = 139 group_id = 1 clientSeq = 61 IfIndex
clientID = 25 group_id = 1 clientSeq = 68 CHKPT RF
clientID = 77 group_id = 1 clientSeq = 84 Event Manager
clientID = 1340 group_id = 1 clientSeq = 101 RP Platform RF
clientID = 1501 group_id = 1 clientSeq = 102 Cat6k CWAN HA
clientID = 78 group_id = 1 clientSeq = 106 TSPTUN HA
clientID = 305 group_id = 1 clientSeq = 107 Multicast ISSU Consolidation RF
clientID = 304 group_id = 1 clientSeq = 108 IP multicast RF Client
clientID = 22 group_id = 1 clientSeq = 109 Network RF Client
clientID = 88 group_id = 1 clientSeq = 110 HSRP
clientID = 114 group_id = 1 clientSeq = 111 GLBP
clientID = 1341 group_id = 1 clientSeq = 114 IOSXE DPIDX
clientID = 1505 group_id = 1 clientSeq = 115 Cat6k SPA TSM
clientID = 75 group_id = 1 clientSeq = 126 Tableid HA
clientID = 71 group_id = 1 clientSeq = 135 XDR RRP RF Client
clientID = 24 group_id = 1 clientSeq = 136 CEF RRP RF Client
clientID = 146 group_id = 1 clientSeq = 138 BFD RF Client
clientID = 301 group_id = 1 clientSeq = 142 MRIB RP RF Client
clientID = 306 group_id = 1 clientSeq = 146 MFIB RRP RF Client
clientID = 1504 group_id = 1 clientSeq = 153 Cat6k CWAN Interface Events
clientID = 402 group_id = 1 clientSeq = 157 TPM RF client
clientID = 520 group_id = 1 clientSeq = 158 RFS RF
clientID = 5 group_id = 1 clientSeq = 160 Config Sync RF client
clientID = 68 group_id = 1 clientSeq = 188 Virtual Template RF Client
clientID = 23 group_id = 1 clientSeq = 191 Frame Relay
clientID = 49 group_id = 1 clientSeq = 192 HDLC
clientID = 72 group_id = 1 clientSeq = 193 LSD HA Proc
clientID = 113 group_id = 1 clientSeq = 194 MFI STATIC HA Proc
clientID = 290 group_id = 1 clientSeq = 195 MPLS TP HA
clientID = 204 group_id = 1 clientSeq = 200 ETHER INFRA RF
clientID = 200 group_id = 1 clientSeq = 203 ETHERNET OAM RF
clientID = 207 group_id = 1 clientSeq = 205 ECFM RF
clientID = 202 group_id = 1 clientSeq = 206 ETHERNET LMI RF
clientID = 206 group_id = 1 clientSeq = 207 BD MAC SECURITY RF CLIENT
clientID = 208 group_id = 1 clientSeq = 208 LLDP
clientID = 226 group_id = 1 clientSeq = 209 LACP
clientID = 229 group_id = 1 clientSeq = 211 ERP
clientID = 20 group_id = 1 clientSeq = 219 IPROUTING NSF RF client
clientID = 100 group_id = 1 clientSeq = 221 DHCPC
clientID = 101 group_id = 1 clientSeq = 222 DHCPD
clientID = 74 group_id = 1 clientSeq = 232 MPLS VPN HA Client
clientID = 34 group_id = 1 clientSeq = 234 SNMP RF Client
clientID = 1502 group_id = 1 clientSeq = 235 CWAN APS HA RF Client
clientID = 52 group_id = 1 clientSeq = 236 ATM
clientID = 116 group_id = 1 clientSeq = 238 CEM
clientID = 117 group_id = 1 clientSeq = 239 IMA
clientID = 69 group_id = 1 clientSeq = 240 AAA
clientID = 123 group_id = 1 clientSeq = 241 SVM HA
clientID = 118 group_id = 1 clientSeq = 242 L2TP
clientID = 119 group_id = 1 clientSeq = 243 XC L2TP HA manager
clientID = 35 group_id = 1 clientSeq = 244 History RF Client
clientID = 90 group_id = 1 clientSeq = 256 RSVP HA Services
clientID = 48 group_id = 1 clientSeq = 266 Dialer
clientID = 250 group_id = 1 clientSeq = 268 EEM Server RF CLIENT
clientID = 252 group_id = 1 clientSeq = 270 EEM POLICY-DIR RF CLIENT
clientID = 54 group_id = 1 clientSeq = 272 SNMP HA RF Client
clientID = 73 group_id = 1 clientSeq = 273 LDP HA
clientID = 76 group_id = 1 clientSeq = 274 IPRM
clientID = 57 group_id = 1 clientSeq = 275 ARP
clientID = 50 group_id = 1 clientSeq = 282 FH_RF_Event_Detect or_stub
clientID = 1342 group_id = 1 clientSeq = 293 IOSXE SpaFlow
clientID = 1343 group_id = 1 clientSeq = 294 IOSXE IF Flow
clientID = 503 group_id = 1 clientSeq = 298 Spanning-Tree Protocol
clientID = 147 group_id = 1 clientSeq = 309 XC RIB MGR
```

```
clientID = 83 group_id = 1 clientSeq = 311 AC RF Client
clientID = 82 group_id = 1 clientSeq = 312 CCM RF
clientID = 145 group_id = 1 clientSeq = 313 VFI Mgr
clientID = 84 group_id = 1 clientSeq = 314 AToM manager
clientID = 85 group_id = 1 clientSeq = 316 SSM
clientID = 280 group_id = 1 clientSeq = 317 XC ST PW OAM
clientID = 212 group_id = 1 clientSeq = 327 REP Protocol
clientID = 105 group_id = 1 clientSeq = 328 DHCP Snooping
clientID = 102 group_id = 1 clientSeq = 332 MQC QoS
clientID = 154 group_id = 1 clientSeq = 333 QoS Feature
clientID = 1510 group_id = 1 clientSeq = 334 Call-Home RF
clientID = 203 group_id = 1 clientSeq = 337 MVRP
clientID = 1601 group_id = 1 clientSeq = 338 TCP
clientID = 1602 group_id = 1 clientSeq = 339 BGP
clientID = 151 group_id = 1 clientSeq = 340 IP Tunnel RF
clientID = 94 group_id = 1 clientSeq = 341 Config Verify RF client
clientID = 130 group_id = 1 clientSeq = 356 CRYPTO RSA
clientID = 131 group_id = 1 clientSeq = 357 PKI RF Client
clientID = 148 group_id = 1 clientSeq = 362 DHCPv6 Relay
clientID = 4005 group_id = 1 clientSeq = 371 ISSU Test Client
clientID = 93 group_id = 1 clientSeq = 375 Network RF 2 Client
clientID = 205 group_id = 1 clientSeq = 377 FEC Client
clientID = 141 group_id = 1 clientSeq = 385 DATA DESCRIPTOR RF CLIENT
clientID = 4006 group_id = 1 clientSeq = 389 Network Clock
clientID = 4022 group_id = 1 clientSeq = 414 IOS Config SHELL
clientID = 4020 group_id = 1 clientSeq = 415 IOS Config ARCHIVE
clientID = 4021 group_id = 1 clientSeq = 416 IOS Config ROLLBACK
clientID = 20001 group_id = 1 clientSeq = 436 License Core HA Client
clientID = 20011 group_id = 1 clientSeq = 437 License Agent HA Client
clientID = 403 group_id = 1 clientSeq = 450 Netsync RF Client
clientID = 15001 group_id = 1 clientSeq = 463 UEA_IOSD_RF_CLIENT
```



CHAPTER 5

Configuring Nonstop Forwarding

This module describes how to configure Nonstop Forwarding (NSF) in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover. NSF is supported by the BGP, EIGRP, IPv6, IS-IS, and OSPF protocols for routing and by CEF for forwarding.

The following terms are used throughout this document:

- NSF-aware device--A device that is running NSF-compatible software
- NSF-capable device--A device that is configured to support NSF. NSF-capable devices can rebuild routing information from either NSF-aware or NSF-capable neighboring devices.

- Prerequisites for Nonstop Forwarding, on page 77
- Restrictions for Nonstop Forwarding, on page 78
- Information About Nonstop Forwarding, on page 79
- How to Configure Nonstop Forwarding, on page 84
- Configuration Examples for Nonstop Forwarding, on page 92
- Additional References, on page 96

Prerequisites for Nonstop Forwarding

- The networking device that is to be configured for NSF must first be configured for SSO. For information, see the Configuring Stateful Switchover section.
- For Border Gateway Protocol (BGP) NSF, all neighboring devices must be NSF-aware and must be configured for BGP graceful restart.
- For Enhanced Interior Gateway Routing Protocol (EIGRP) NSF:
  - All neighboring devices must be NSF-capable or NSF-aware.
  - An NSF-aware device must be completely converged with the network before it can assist an NSF-capable device in an NSF restart operation.
- For Internet Engineering Task Force (IETF) Intermediate System to Intermediate System (IS-IS), all neighboring devices must be NSF-aware.
- For Open Shortest Path First (OSPF) NSF, all networking devices on the same network segment must be NSF-aware.

- For IPv6 NSF, IPv6 must be enabled on your networking device.
- On platforms supporting the Route Switch Processor (RSP), and where the Cisco Express Forwarding (CEF) switching mode is configurable, configure distributed CEF (dCEF) switching mode using the **ip cef distributed** command.

Restrictions for Nonstop Forwarding

General Restrictions

NSF capability is not enabled by default for OSPF, ISIS, or BGP. NSF capability is enabled by default for EIGRP only.

BGP NSF Restrictions

- BGP support in NSF requires that neighbor networking devices be NSF-aware. If an NSF-capable device discovers that a particular BGP neighbor does not have graceful restart capability, it will not establish an NSF-capable session with that neighbor. All other neighbors that have graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device.
- All devices must be configured with the same type of NSF helper mode, either IETF graceful restart or Cisco NSF.

EIGRP NSF Restrictions

- An NSF-aware device cannot support two NSF-capable peers performing an NSF restart operation at the same time. However, both neighbors will reestablish peering sessions after the NSF restart operation is complete.
- Distributed platforms that run a supporting version of Cisco software can support full NSF capabilities. These devices can perform a restart operation and can support other NSF capable peers.
- Single processor platforms that run a supporting version of Cisco software support only NSF awareness. These devices maintain adjacency and hold known routes for the NSF-capable neighbor until it signals that it is ready for the NSF-aware device to send its topology table or the route-hold timer expires.

OSPF NSF Restrictions

- OSPF NSF for virtual links is not supported.
- OSPF NSF for sham links is not supported.
- OSPF NSF supports NSF/SSO for IPv4 traffic only.
- OSPFv3 is not supported with NSF/SSO. Only OSPFv2 is supported with NSF/SSO.
- All neighbor networking devices must be NSF-aware. If an NSF-capable device discovers that it has non-NSF-aware neighbors on a particular network segment, it will disable NSF capabilities for that

segment. Other network segments composed entirely of NSF-capable or NSF-aware devices will continue to provide NSF capabilities.

- You can configure strict link state advertisement (LSA) checking on both NSF-aware and NSF-capable devices; however, it is effective only when the device is in helper mode.

Information About Nonstop Forwarding

Nonstop Forwarding



Note In the following content, the term Route Processor (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted.

NSF works with the SSO feature in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following an RP switchover.

Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

The NSF feature provides the following benefits:

- Improved network availability—NSF continues forwarding network traffic and application state information so that user session information is maintained after a switchover.
- Overall network stability—Network stability may be improved with the reduction in the number of route flaps that had been created when devices in the network failed and lost their routing tables.
- Neighboring devices do not detect link flapping—Because the interfaces remain up across a switchover, neighboring devices do not detect a link flap (that is, the link does not go down and come back up).
- Prevention of routing flaps—Because SSO continues forwarding network traffic in the event of a switchover, routing flaps are avoided.
- No loss of user sessions—User sessions established prior to the switchover are maintained.

NSF always runs together with SSO. SSO supported protocols and applications must be high-availability (HA)-aware. A feature or protocol is HA-aware if it maintains, either partially or completely, undisturbed operation during an RP switchover. For some HA-aware protocols and applications, state information is synchronized from the active to the standby processor.

Cisco NSF Routing and Forwarding

Cisco NSF is supported by the BGP, EIGRP, IPv6, IS-IS, and OSPF protocols for routing and by CEF for forwarding. Of the routing protocols, BGP, EIGRP, IPv6, IS-IS, and OSPF have been enhanced with NSF-capability and awareness, which means that devices running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices. The IS-IS protocol can be configured to use state information that has been synchronized between the active and the standby RP to recover route information following a switchover instead of information received from peer devices.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

Cisco Express Forwarding and NSF

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates to CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

The routing protocols run only on the active RP, and they receive routing updates from their neighbor devices. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables. Alternately, the IS-IS protocol can be configured to synchronize state information from the active to the standby RP to help rebuild the routing table on the NSF-capable device in environments where neighbor devices are not NSF-aware.

For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information. The CEF NSF feature operates by default while the networking device is running in SSO mode. No configuration is necessary.

BGP NSF Operations

When a NSF-capable device begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a declaration that the NSF-capable device has “graceful restart capability.” Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the

NSF-capable device and its BGP peers need to exchange the graceful restart capability in their OPEN messages, at the time of session establishment. If both the peers do not exchange the graceful restart capability, the session will not be graceful restart capable.

If the BGP session is lost during the RP switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable device as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the NSF-capable device reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable device as having restarted.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding information. The NSF-aware device uses the network information to remove stale routes from its BGP table. Following that, the BGP protocol is fully converged.

If a BGP peer does not support the graceful restart capability, it will ignore the graceful-restart capability in an OPEN message but will establish a BGP session with the NSF-capable device. This function will allow interoperability with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware BGP peers will not be graceful restart-capable.

BGP support in NSF requires that neighbor networking devices be NSF-aware; that is, the devices must have the graceful restart capability and advertise that capability in their OPEN message during session establishment. If an NSF-capable device discovers that a particular BGP neighbor does not have graceful restart capability, it will not establish an NSF-capable session with that neighbor. All other neighbors that have graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device.

EIGRP NSF Operations

Cisco NSF is supported by the EIGRP protocol for routing and by CEF for forwarding. EIGRP depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

EIGRP nonstop forwarding (NSF) capabilities are exchanged by EIGRP peers in hello packets. The NSF-capable device notifies its neighbors that an NSF restart operation has started by setting the restart (RS) bit in a hello packet. When an NSF-aware device receives notification from an NSF-capable neighbor that an NSF-restart operation is in progress, the NSF-capable and NSF-aware devices immediately exchange their topology tables. The NSF-aware device sends an end-of-table (EOT) update packet when the transmission of its topology table is complete. The NSF-aware device then performs the following actions to assist the NSF-capable device:

- The EIGRP hello hold timer is expired to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware device to reply to the NSF-capable device more quickly reducing the amount of time required for the NSF-capable device to rediscover neighbors and rebuild the topology table.
- The route-hold timer is started. This timer is used to set the period of time that the NSF-aware device will hold known routes for the NSF-capable neighbor.
- The NSF-aware device notes in the peer list that the NSF-capable neighbor is restarting, maintains adjacency, and holds known routes for the NSF-capable neighbor until the neighbor signals that it is ready for the NSF-aware device to send its topology table or the route-hold timer expires. If the route-hold

timer expires on the NSF-aware device, the NSF-aware device will discard held routes and treat the NSF-capable device as a new device joining the network and reestablishing adjacency accordingly.

- The NSF-aware device will continue to send queries to the NSF-capable device that is still converging after switchover, effectively extending the time before a stuck-in-active (SIA) condition can occur.

When the switchover operation is complete, the NSF-capable device notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting devices. The NSF-capable device then returns to normal operation. The NSF-aware device will look for alternate paths (go active) for any routes that are not refreshed by the NSF-capable (restarting device). The NSF-aware device will then return to normal operation. If all paths are refreshed by the NSF-capable device, the NSF-aware device will immediately return to normal operation.

NSF-aware devices are completely compatible with non-NSF-aware or non-NSF-capable neighbors in an EIGRP network. A non-NSF-aware neighbor will ignore NSF capabilities and reset adjacencies and otherwise maintain the peering sessions normally.

IPv6 support for NSF Operations

Nonstop Forwarding and Graceful Restart for MP-BGP IPv6 Address Family

The graceful restart capability is supported for IPv6 BGP unicast, multicast, and VPNv6 address families, enabling Cisco NSF functionality for BGP IPv6. The BGP graceful restart capability allows the BGP routing table to be recovered from peers without keeping the TCP state.

NSF continues forwarding packets while routing protocols converge, therefore avoiding a route flap on switchover. Forwarding is maintained by synchronizing the FIB between the active and standby RP. On switchover, forwarding is maintained using the FIB. The RIB is not kept synchronized; therefore, the RIB is empty on switchover. The RIB is repopulated by the routing protocols and subsequently informs the FIB about RIB convergence by using the NSF_RIB_CONVERGED registry call. The FIB tables are updated from the RIB, removing any stale entries. The RIB starts a fail-safe timer during RP switchover, in case the routing protocols fail to notify the RIB of convergence.

The Cisco BGP address family identifier (AFI) model is modular and scalable, and supports multiple AFIs and subsequent address family identifier (SAFI) configurations.

Nonstop Forwarding for IPv6 RIP

RIP registers as an IPv6 NSF client. Doing so has the benefit of using RIP routes installed in the Cisco Express Forwarding table until RIP has converged on the standby.

Nonstop Forwarding for Static Routes

Cisco NSF supports IPv6 static routes.

IS-IS NSF Operations

When an IS-IS NSF-capable device performs an RP switchover, it must perform two tasks in order to resynchronize its Link State Database with its IS-IS neighbors. First, it must relearn the available IS-IS neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the Link State Database for the network.

The IS-IS NSF feature offers two options when configuring NSF:

- IETF IS-IS
- Cisco IS-IS

If neighbor devices on a network segment are NSF-aware, meaning that neighbor devices are running a software version that supports the IETF Internet draft for device restartability, they will assist an IETF NSF device that is restarting. With IETF, neighbor devices provide adjacency and link-state information to help rebuild the routing information following a switchover. A benefit of IETF IS-IS configuration is operation between peer devices based on a proposed standard.

If you configure IETF on the networking device, but neighbor devices are not IETF-compatible, NSF will cancel following a switchover.

If the neighbor devices on a network segment are not NSF-aware, you must use the Cisco configuration option. The Cisco IS-IS configuration transfers both protocol adjacency and link-state information from the active to the standby RP. A benefit of Cisco configuration is that it does not rely on NSF-aware neighbors.

IETF IS-IS Configuration

With the IETF IS-IS configuration, the NSF-capable device sends IS-IS NSF restart requests to neighboring NSF-aware devices as quickly as possible after an RP switchover. Neighbor networking devices recognize this restart request as a cue that the neighbor relationship with this device should not be reset, but that they should initiate database resynchronization with the restarting device. As the restarting device receives restart request responses from devices on the network, it can begin to rebuild its neighbor list.

Once this exchange is complete, the NSF-capable device uses the link-state information to remove stale routes, update the RIB, and update the FIB with the new forwarding information. IS-IS is then fully converged.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. The IS-IS NSF operation waits for a specified interval to ensure that connections are stable before attempting another restart of IS-IS NSF. This functionality prevents IS-IS from attempting back-to-back NSF restarts with stale information.

Cisco IS-IS Configuration

With the Cisco configuration option, full adjacency and link-state packet (LSP) information is saved, or “checkpointed,” to the standby RP. Following a switchover, the newly active RP maintains its adjacencies using the checkpointed data, and can quickly rebuild its routing tables.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. Once this synchronization is completed, IS-IS adjacency and LSP data is checkpointed to the standby RP; however, a new NSF restart will not be attempted by IS-IS until the interval time expires. This functionality prevents IS-IS from attempting back-to-back NSF restarts. IS-IS NSF provides a command to extend the wait time for interfaces that, for whatever reason, do not come up in a timely fashion.

Following a switchover, Cisco IS-IS NSF has complete neighbor adjacency and LSP information; however, it must wait for all interfaces that had adjacencies prior to the switchover to come up. If an interface does not come up within the allocated interface wait time, the routes learned from these neighbor devices are not considered in routing table recalculation.

NSF-OSPF Operations

For Cisco Nonstop Forwarding (NSF), the Open Shortest Path First (OSPF) routing protocol has been enhanced to support high availability (HA) features in Stateful Switchover (SSO). Before an OSPF NSF-capable device can perform a Route Processor (RP) switchover, the device must be aware of the available OSPF neighbors on the network without resetting the neighbor relationship, and the device must acquire the contents of the link state database for the network. The NSF-capable device sends an OSPF NSF signal to neighboring NSF-aware devices to notify the devices that the neighbor relationship with the sending device must not be reset. The NSF-capable device uses the signals that it receives from other devices on the network to rebuild its neighbor list.

The NSF-capable device synchronizes its database with all the NSF-aware neighbors on its neighbor list. After all neighbors exchange routing information, the NSF-capable device uses the routing information to remove stale routes and update the routing information base (RIB) and the forwarding information base (FIB) with the new forwarding information. The OSPF protocols are then fully converged.

Prior to RFC 3623, Cisco implemented the proprietary Cisco NSF. The RFC 3623 Graceful OSPF Restart feature supports IETF NSF for OSPF processes in multivendor networks. The following are NSF device modes of operation common to Cisco and IETF NSF implementations:

- Restarting mode—In this mode, the OSPF device performs nonstop forwarding recovery because of an RP switchover.
- Helper mode—Also known as NSF-awareness mode. In this mode, the neighboring device is in the restarting state and helps in NSF recovery.

The strict link state advertisement (LSA) checking feature allows a helper device to terminate the graceful restart process if the device detects a changed LSA that would cause flooding during the graceful restart process. Strict LSA checking is disabled by default. You can enable strict LSA checking when there is a change to an LSA that would be flooded to the restarting device.

How to Configure Nonstop Forwarding

Configuring and Verifying BGP NSF

Repeat this procedure on each peer device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 120`	Enables a BGP routing process, and enters router configuration mode.
Step 4	**bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] **Example:** `Router(config-router)# bgp graceful-restart`	Enables the BGP graceful restart capability, which starts NSF for BGP.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 6	**show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy**[**detail**]]] **Example:** `Router# show ip bgp neighbors`	Displays information about BGP and TCP connections to neighbors.

Configuring and Verifying EIGRP NSF

Repeat this procedure on each peer device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:**	Enables an EIGRP routing process, and enters router configuration mode.

	Command or Action	Purpose
	`Router(config)# router eigrp 109`	
Step 4	**nsf** **Example:** `Router(config)# no nsf`	(Optional) Enables NSF capabilities. • This command is enabled by default.
Step 5	**timers nsf converge** *seconds* **Example:** `Router(config-router)# timers nsf converge 120`	(Optional) Adjusts the maximum time that the restarting device will wait for the EOT notification from an NSF-capable or NSF-aware peer. • Enter this command on NSF-capable devices only.
Step 6	**timers nsf signal** *seconds* **Example:** `Router(config-router)# timers nsf signal 20`	(Optional) Adjusts the maximum time for the initial restart period. • Enter this command on NSF-capable devices only.
Step 7	**timers nsf route-hold** *seconds* **Example:** `Router(config-router)# timers nsf route-hold 240`	(Optional) Sets the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer.
Step 8	**timers graceful-restart purge-time** *seconds* **Example:** `Router(config-router)# timers graceful-restart purge-time 240`	(Optional) Sets the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer.
Step 9	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 10	**show ip protocols** **Example:** `Router# show ip protocols`	Displays the parameters and current state of the active routing protocol process.

Configuring NSF-OSPF

Perform only one of the following tasks:

Configuring Cisco NSF-OSPF

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 12`	Enables Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf cisco** [**enforce global**] **Example:** `Device(config-router)# nsf cisco`	Enables Cisco Nonstop Forwarding (NSF) restarting mode. • This command is not required on devices that operate only in NSF helper mode.
Step 5	**nsf cisco helper** [**disable**] **Example:** `Device(config-router)# nsf cisco helper`	Enables Cisco NSF helper support. • This command shows how to enable Cisco NSF helper mode.
Step 6	**nsf ietf helper** [**disable** | **strict-lsa-checking**] **Example:** `Device(config-router)# nsf ietf helper disable`	(Optional) Disables IETF NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** `Device# show ip ospf nsf`	Displays OSPF NSF state information.

Configuring IETF NSF-OSPF

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 12`	Enables Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf ietf** [**restart-interval** *seconds*] **Example:** `Device(config-router)# nsf ietf restart-interval 180`	Enables IETF Nonstop Forwarding (NSF) restarting mode. • This command is not required on devices that operate only in helper mode.
Step 5	**nsf ietf helper** [**disable** | **strict-lsa-checking**] **Example:** `Device(config-router)# nsf ietf helper strict-lsa-checking`	(Optional) Configures IETF NSF helper mode on neighbor devices that operate in helper mode.
Step 6	**nsf cisco helper disable** **Example:** `Device(config-router)# nsf cisco helper disable`	(Optional) Disables Cisco NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** `Device# show ip ospf nsf`	Displays OSPF NSF state information.

Configuring and Verifying IS-IS NSF

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis cisco1`	Enables the IS-IS routing protocol to specify an IS-IS process and enters router configuration mode.
Step 4	**nsf** [**cisco** | **ietf**] **Example:** `Router(config-router)# nsf ietf`	Enables IS-IS NSF operations.
Step 5	**nsf interval** *minutes* **Example:** `Router(config-router)# nsf interval 2`	(Optional) Configures the minimum time between NSF restart attempts.
Step 6	**nsf t3** {**manual** *seconds* | **adjacency**} **Example:** `Router(config-router)# nsf t3 manual 40`	(Optional) Specifies the methodology used to determine how long IETF NSF will wait for the link-state packet (LSP) database to synchronize before generating overloaded link-state information. • This command is supported for IETF NSF only.
Step 7	**nsf interface wait** *seconds* **Example:** `Router(config-router)# nsf interface wait 15`	(Optional) Specifies how long a Cisco NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart. • This command is supported for Cisco NSF only.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 9	**show isis nsf** **Example:** `Router# show isis nsf`	Displays current state information regarding IS-IS NSF.

Troubleshooting Nonstop Forwarding

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eigrp nsf** **Example:** `Device# debug eigrp nsf`	Displays notifications and information about NSF events for an EIGRP routing process.
Step 3	**debug ip eigrp notifications** **Example:** `Device# debug ip eigrp notifications`	Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.
Step 4	**debug isis nsf** [**detail**] **Example:** `Device# debug isis nsf [detail]`	Displays information about the IS-IS state during a Cisco NSF restart.
Step 5	**debug ospf nsf** [**detail**] **Example:** `Device# debug ospf nsf [detail]`	Displays debugging messages related to OSPF Cisco NSF commands.
Step 6	**show cef nsf** **Example:** `Device# show cef nsf`	Displays the current NSF state of CEF on both the active and standby RPs.

	Command or Action	Purpose
Step 7	**show cef state** **Example:** `Device# show cef state`	Displays the CEF state on a networking device.
Step 8	**show clns neighbors** **Example:** `Device# show clns neighbors`	Displays both end system and intermediate system neighbors.
Step 9	**show ip bgp** **Example:** `Device# show ip bgp`	Displays entries in the BGP routing table.
Step 10	**show ip bgp neighbor** **Example:** `Device# show ip bgp neighbor`	Displays information about the TCP and BGP connections to neighbor devices.
Step 11	**show ip cef** **Example:** `Device# show ip cef`	Displays entries in the FIB that are unresolved, or displays FIB summary.
Step 12	**show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**] **Example:** `Device# show ip eigrp neighbors detail`	Displays displayed information about neighbors discovered by EIGRP.
Step 13	**show ip ospf** **Example:** `Device# show ip ospf`	Displays general information about OSPF routing processes.
Step 14	**show ip ospf neighbor** [**detail**] **Example:** `Device# show ip ospf neighbor [detail]`	Displays OSPF-neighbor information on a per-interface basis.
Step 15	**show ip protocols** **Example:** `Device# show ip protocols`	Displays the parameters and current state of the active routing protocol process. • The status of EIGRP NSF configuration and support is displayed in the output.

	Command or Action	Purpose
Step 16	**show isis database** [**detail**] **Example:** `Device# show isis database [detail]`	Displays the IS-IS link-state database.
Step 17	**show isis nsf** **Example:** `Device# show isis nsf`	Displays the current state information regarding IS-IS NSF.

Configuration Examples for Nonstop Forwarding

Example NSF-Capable CEF

The CEF NSF feature operates by default while the router is running in SSO mode. No configuration is necessary. The following sample output shows that CEF is NSF capable:

```
Router# show cef state
CEF Status:
 RP instance
 common CEF enabled
IPv4 CEF Status:
 CEF enabled/running
 dCEF enabled/running
 CEF switching enabled/running
 universal per-destination load sharing algorithm, id 91429870
IPv6 CEF Status:
 CEF enabled/running
 dCEF enabled/running
 universal per-destination load sharing algorithm, id 91429870
RRP state:
 I am standby RRP:                  no
 RF Peer Presence:                  yes
 RF Peer Comm reached:              yes
 RF Peer Config done:               yes
 RF Progression blocked:            never
 Redundancy mode:                   sso(3)
 CEF NSF sync:                      enabled/running

CEF ISSU Status:
  FIBHWIDB broker
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
  FIBIDB broker
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
  FIBHWIDB Subblock broker
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
  FIBIDB Subblock broker
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
  Adjacency update
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
  IPv4 table broker
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
  IPv6 table broker
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
```

```
  CEF push
    Slot(s): 7 (0x80) (grp 0x3FBE6360) - Nego compatible.
```

Example BGP NSF

The following partial output shows the BGP configuration on the SSO-enabled device:

```
Router# show running-config
router bgp 120
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
```

The following sample output shows that the graceful restart function is both advertised and received and that the address families have the graceful restart capability. If no address families were listed, then BGP NSF will not occur.

```
Router# show ip bgp neighbors
 192.168.2.2
BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
Address family IPv4 Unicast:advertised and received
    Address family IPv4 Multicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

Example: EIGRP NSF

The following sample output shows that EIGRP NSF support is present in the installed software image.

- “EIGRP NSF-aware route hold timer is . . .” is displayed in the output for either NSF-aware or NSF-capable devices, and the default or user-defined value for the route-hold timer is displayed.
- “EIGRP NSF enabled” or “EIGRP NSF disabled” appears in the output only when the NSF capability is supported by the device.

```
Device# show ip protocols

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
```

```
    NSF signal timer is 20s
    NSF converge timer is 120s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

Example: Configuring Cisco NSF-OSPF

The following example shows how to enable Cisco Nonstop Forwarding (NSF) helper support in the router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 400
Device(config-router)# nsf cisco helper
Device(config-router)# nsf ietf helper disable
Device(config-router)# end
```

The following sample output from the **show ip ospf nsf** command shows that NSF is enabled for Open Shortest Path First (OSPF) process 400. NSF helper mode is enabled by default on devices running NSF-compatible software. In this configuration, IETF helper mode is disabled for process 400.

```
Device> show ip ospf nsf

Routing Process "ospf 400"
Non-Stop Forwarding enabled
IETF NSF helper support disabled
Cisco NSF helper support enabled
  OSPF restart state is NO_RESTART
  Handle 2162698, Router ID 192.168.2.155, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Example: Configuring IETF NSF-OSPF

The following example shows how to enable IETF Nonstop Forwarding (NSF) helper support in the router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 500
Device(config-router)# nsf ietf helper strict-lsa-checking
Device(config-router)# nsf cisco helper disable
Device(config-router)# end
```

The following sample output from the **show ip ospf nsf** command shows that NSF is enabled for Open Shortest Path First (OSPF) process 500. NSF helper mode is enabled by default on devices running NSF-compatible software. In this configuration, Cisco helper mode is disabled.

```
Device> show ip ospf nsf

Routing Process "ospf 500"
Non-Stop Forwarding enabled
```

```
IETF NSF helper support enabled
Cisco NSF helper support disabled
  OSPF restart state is NO_RESTART
  Handle 1786466333, Router ID 10.1.1.1, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Example IS-ISNSF

The following partial output shows that this device uses the Cisco implementation of IS-IS NSF. The display will show either Cisco IS-IS or IETF IS-IS configuration.

```
Router# show running-config
router isis
nsf cisco
```

In a Cisco NSF configuration, the display output is different on the active and the standby RPs.

The following sample output on the active RP shows that Cisco NSF is enabled on the device:

```
Router# show isis nsf
NSF is ENABLED, mode 'cisco'
RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

The following sample output on the standby RP shows that NSF is enabled on the device (NSF restart enabled):

```
Router# show isis nsf
NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

The following sample output shows that IETF NSF is configured for the IS-IS networking device:

```
Router# show isis nsf
NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
```

```
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS master command list	Cisco IOS Master Command List , All Releases
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

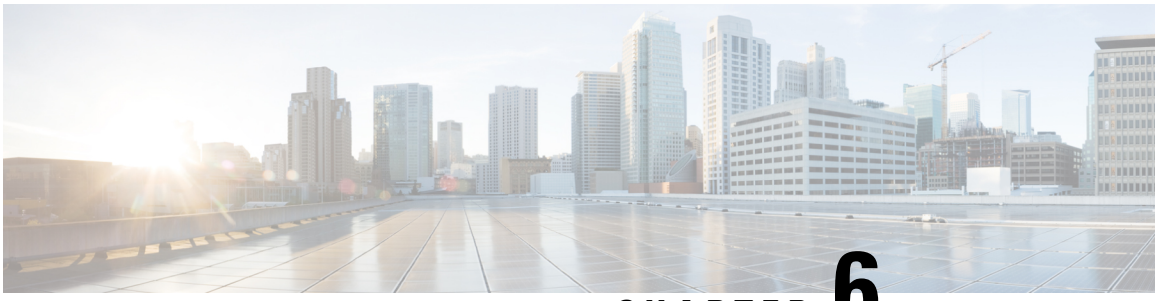
MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified. Cisco ASR 900 Series Aggregation Services Routers MIB Specifications Guide	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs Cisco ASR 900 Series Aggregation Services Routers MIB Specifications Guide

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 6

Performing an In Service Software Upgrade

In Service Software Upgrade (ISSU) allows Cisco software to be upgraded or downgraded, at a router level, while the system continues to forward packets. ISSU takes advantage of the Cisco high availability infrastructure--Cisco NSF with SSO and hardware redundancy--and eliminates downtime that is associated with software upgrades or version changes by allowing updates while the system remains in service. Cisco high availability features combine to lower the impact that planned maintenance activities have on network service availability, with the results of less downtime and better access to critical systems.

SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two Route Processors (RPs) to remain synchronized although they may support different sets of commands.

An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, you must copy the Cisco IOS software into the file systems of both RPs.

After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP.

After switchover, the standby RP takes over as the new active RP.

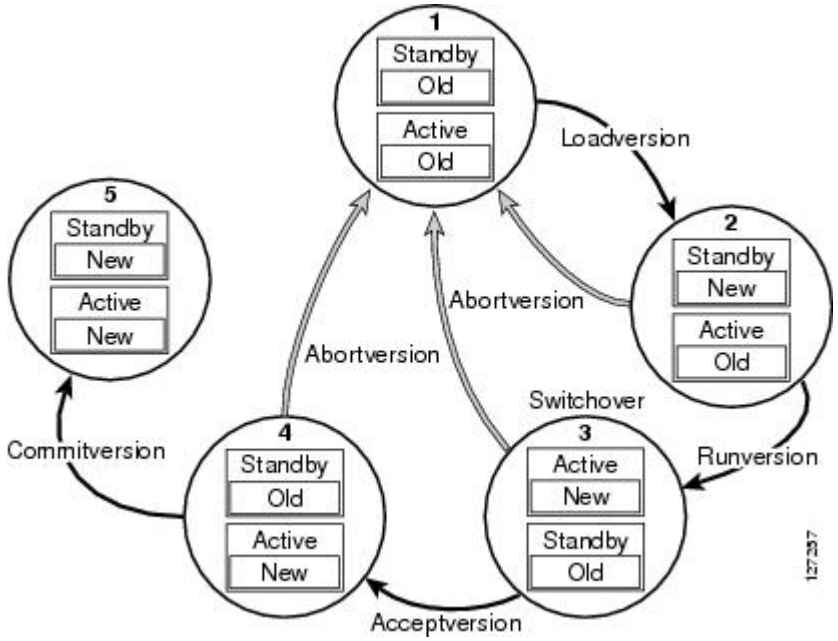
Then, the former active RP, which is now the new standby RP, is loaded with the new software.

The two RPs in a system can be in one of three different states during ISSU:

- Active--One RP is actively forwarding packets with old software. After the ISSU process is performed, the original active RP becomes the standby RP.
- Standby--Perform ISSU on the standby RP, loading it with new software. After the ISSU process is performed, the original standby RP is the new active RP.
- Hot standby--After the original standby RP becomes the new active RP, load the new software image into the new standby RP. Doing so makes the standby RP a hot standby RP.

The following figure shows the ISSU states during the ISSU process.

Figure 3: ISSU States During the ISSU Process



Caution If you downgrade from release 16.10 and later to any previous releases of 16.9 and earlier, irrespective of whether a port-channel with 16 member-link is configured or not, you must configure and save by using the **port-channel max-memlink-per-pc 8** command, before you proceed to perform ISSU (downgrade).