



## Cisco IOS XE High Availability Configuration Guide

Release 2

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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

*Cisco IOS XE High Availability Configuration Guide*  
© 2009 Cisco Systems, Inc. All rights reserved.



# Cisco High Availability Features Roadmap

---

**First Published:** December 31, 2007  
**Last Updated:** December 4, 2010

This feature roadmap lists the Cisco IOS XE features documented in the *Cisco IOS XE High Availability Configuration Guide* and maps them to the documents in which they appear. The roadmap is organized so that you can select your release train and see the features in that release. Find the feature name you are searching for and click on the URL in the “Where Documented” column to access the document containing that feature.

Many legacy features have been incorporated into the configuration files, and these features may not have entries in this roadmap. For the latest feature information and caveats, see the release notes for your platform and software release.

## Feature and Release Support

**Table 1** lists High Availability feature support for the following Cisco IOS XE software release trains:

- [Cisco IOS XE Release 3.1S](#)
- [Cisco IOS XE Release 2.5](#)
- [Cisco IOS XE Release 2.3](#)
- [Cisco IOS XE Release 2.1](#)

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

---

**Table 1** lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

---

**Table 1** lists the most recent release of each software train first and the features in alphabetical order within the release.



---

Americas Headquarters:  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007–2010 Cisco Systems, Inc. All rights reserved.

Table 1 Supported High Availability Features

Release	Feature Name	Feature Description	Where Documented
Cisco IOS XE Release 2.1			
Cisco IOS XE Release 2.1	AAA High Availability Support for Local PPPoX Sessions	This feature enhances the authentication, authorization, and accounting (AAA) capability to meet high availability (HA) criteria for locally terminated Point-to-Point Protocol (PPP) over Ethernet (PPPoE) and PPPoEoX sessions, where X represents VLAN, or QinQ.	<a href="#">AAA High Availability Support for Local PPPoX Sessions</a>
	Dual Cisco IOS processes on the same RP	This feature allows a standby IOS process to be available on the same Route Processor as the active IOS process. This standby IOS process can be switched to in the event of an IOS failure, and can also be used to upgrade sub-package software in some scenarios as the standby IOS process in an ISSU upgrade. On the Cisco ASR 1000 Series Routers, IOS runs as one of many processes within the operating system.	<a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</a>
	Enhanced SNMP Support for High Availability	The Enhanced SNMP Support for High Availability feature provides support for managing a networking device running stateful switchover (SSO). This document describes the enhancements and modifications made to the Cisco IOS Simple Network Management Protocol (SNMP) infrastructure to support SSO for Route Processors (RPs).	<a href="#">Configuring Stateful Switchover</a>
	IPv6: Base protocols high availability	This feature extends high availability (HA) features, nonstop forwarding and stateful switchover (NSF/SSO) and In Service Software Upgrade (ISSU), functionality to IPv6 protocols and applications.	<a href="#">Implementing IPv6 Addressing and Basic Connectivity</a>
	IPv6: NSF 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 nonstop forwarding (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.	<a href="#">Implementing Multiprotocol BGP for IPv6</a>

**Table 1 Supported High Availability Features (continued)**

Release	Feature Name	Feature Description	Where Documented
Cisco IOS XE Release 2.1	IPv6: RIPv6 Nonstop Forwarding	IPv6 Routing Information Protocol (RIP) supports nonstop forwarding (NSF). 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.	<a href="#">Implementing RIP for IPv6</a>
	IPv6: Static Route Nonstop Forwarding	IPv6 static routes support Cisco nonstop forwarding (NSF). NSF continues forwarding packets while routing protocols converge, therefore avoiding a route flap on switchover.	<a href="#">Implementing Static Routes for IPv6</a>
	ISSU	The In Service Software Upgrade (ISSU) feature allows Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS XE software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - ARP	This feature provides In Service Software Upgrade (ISSU) support for Address Resolution Protocol High Availability.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - Frame Relay	This feature delivers In Service Software Upgrade (ISSU) support for Frame Relay connections during a planned software upgrade on a dual-RP HA platform utilizing ISSU capability.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - GLBPv6	This feature delivers In Service Software Upgrade (ISSU) support for GLBPv6	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - HDLC	This feature provides In Service Software Upgrade (ISSU) support for the High-Level Data Link Control (HDLC) protocol.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - HSRPv6	This feature provides In Service Software Upgrade (ISSU) support for Hot Standby Router Protocol for IPv6 (HSRPv6).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - IGMP snooping	This feature adds In Service Software Upgrade (ISSU) support for Internet Group Management Protocol (IGMP) Snooping.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - IPv6 uRPF	This feature adds In Service Software Upgrade (ISSU) support for IPv6 Unicast Reverse Path Forwarding (uRPF).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>

Table 1 Supported High Availability Features (continued)

Release	Feature Name	Feature Description	Where Documented
Cisco IOS XE Release 2.1	ISSU - IS-IS	This feature adds In Service Software Upgrade (ISSU) support for the Intermediate System-to-Intermediate System (IS-IS) protocol.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - Managed LNS MPLS	This feature adds In Service Software Upgrade (ISSU) support for Managed L2TP network server (LNS) Multiprotocol Label Switching Protocol (MPLS), also known as VRF-Lite MPLS.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - MLD Access Group	This feature adds In Service Software Upgrade (ISSU) support for Multicast Listener Discovery Protocol (ML) access groups.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - Multicast MPLS VPN	This feature adds In Service Software Upgrade (ISSU) support for multicast Multiprotocol Label Switching Protocol (MPLS) Virtual Private Networks (VPNs).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - NAT	This feature adds In Service Software Upgrade (ISSU) support for Network Address Translation (NAT).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - PPP/MLP	This feature adds In Service Software Upgrade (ISSU) support for Point-to-Point Protocol/Multilink PPP (PPP/MLP).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - QoS	This feature provides In Service Software Upgrade (ISSU) support for quality of service (QoS).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	ISSU - SNMP	This feature adds In Service Software Upgrade (ISSU) support for the Simple Network Management Protocol (SNMP).	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	NSF Awareness (Nonstop Forwarding Awareness)	The NSF Awareness feature provides Nonstop Forwarding (NSF) support for routing protocols—Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS).	<a href="#">Configuring Nonstop Forwarding</a>
	NSF Awareness - EIGRP	This feature provides Nonstop Forwarding (NSF) support for Enhanced Interior Gateway Routing Protocol (EIGRP).	<a href="#">Configuring Nonstop Forwarding</a>
	NSF - BGP	This feature provides Border Gateway Protocol (BGP) support for Nonstop Forwarding (NSF).	<a href="#">Configuring Nonstop Forwarding</a>
	NSF - EIGRP	This feature provides Enhanced Interior Gateway Routing Protocol (EIGRP) support for Nonstop Forwarding (NSF).	<a href="#">Configuring Nonstop Forwarding</a>

Table 1 Supported High Availability Features (continued)

Release	Feature Name	Feature Description	Where Documented
Cisco IOS XE Release 2.1	NSF - IS-IS	This feature provides Intermediate System-to-Intermediate System (IS-IS) support for Nonstop Forwarding (NSF).	<a href="#">Configuring Nonstop Forwarding</a>
	NSF - OSPF	This feature adds Open Shortest Path First (OSPF) support for high availability (HA) Nonstop Forwarding (NSF).	<a href="#">Configuring Nonstop Forwarding</a>
	NSF—OSPF (RFC 3623) OSPF Graceful Restart	This document focuses on nonstop forwarding (NSF) for OSPFv2 in Cisco IOS XE software, using the IETF standardized graceful restart functionality as described in RFC 3623.	<a href="#">Configuring Nonstop Forwarding</a>
	NSF/SSO - GLBPv6	<ul style="list-style-type: none"> <li>This feature provides high availability (HA) support for Cisco Gateway Load Balancing Protocol Version 6 (GLBPv6).</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Configuring Nonstop Forwarding</a></li> <li><a href="#">Configuring Stateful Switchover</a></li> </ul>
	NSF/SSO - HSRPv6	This feature provides high availability (HA) support for Hot Standby Router Protocol Version 6 (HSRPv6).	<ul style="list-style-type: none"> <li><a href="#">Configuring Nonstop Forwarding</a></li> <li><a href="#">Configuring Stateful Switchover</a></li> </ul>
	NSF/SSO - IPsec	This feature provides high availability (HA) support for IP security (IPsec).	<ul style="list-style-type: none"> <li><a href="#">Configuring Nonstop Forwarding</a></li> <li><a href="#">Configuring Stateful Switchover</a></li> </ul>
	NSF/SSO - IPv6 uRPF	This feature provides high availability (HA) support for IPv6 Unicast Reverse Path Forwarding (uRPF).	<ul style="list-style-type: none"> <li><a href="#">Configuring Nonstop Forwarding</a></li> <li><a href="#">Configuring Stateful Switchover</a></li> </ul>
	NSF/SSO - Managed LNS MPLS	This feature provides high availability (HA) support for Managed L2TP network server (LNS) Multiprotocol Label Switching Protocol (MPLS), also known as VRF-Lite MPLS.	<ul style="list-style-type: none"> <li><a href="#">Configuring Nonstop Forwarding</a></li> <li><a href="#">Configuring Stateful Switchover</a></li> </ul>
	NSF/SSO - MLD Access Group	This feature provides high availability (HA) support for Multicast Listener Discovery Protocol (MLD) Access Group.	<ul style="list-style-type: none"> <li><a href="#">Configuring Nonstop Forwarding</a></li> <li><a href="#">Configuring Stateful Switchover</a></li> </ul>
	NSF/SSO—MPLS VPN	This feature allows a provider edge (PE) router (with redundant Route Processors) to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor restarts.	<a href="#">Configuring NSF/SSO—MPLS VPN</a>

Table 1 Supported High Availability Features (continued)

Release	Feature Name	Feature Description	Where Documented
Cisco IOS XE Release 2.1	NSF/SSO (Nonstop Forwarding with Stateful Switchover)	Cisco Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) feature in Cisco IOS XE Software. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. Stateful Switchover (SSO) maintains the layer two connectivity protocols between devices while Nonstop Forwarding (NSF) continues to forward IP packets during the route convergence time. The result is a transparent Route Processor (RP) failure; there are no loss sessions or route flaps in the network.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Nonstop Forwarding</a></li> <li>• <a href="#">Configuring Stateful Switchover</a></li> </ul>
	SSO - Frame Relay	This feature provides stateful switchover (SSO) support for Frame Relay. With SSO, Frame Relay dynamic state information is synchronized between the active Route Processor (RP) and standby RP.	<a href="#">Configuring Stateful Switchover</a>
	SSO - GLBP	This feature provides stateful switchover (SSO) support for the Cisco Gateway Load Balancing Protocol (GLBP). With SSO, GLBP can detect when a router is failing over to the secondary Route Processor (RP) and continue in its current GLBP group state.	<a href="#">Configuring Stateful Switchover</a>
	SSO - HDLC	This feature provides stateful switchover (SSO) support for High-Level Data Link Control (HDLC). HDLC SSO will synchronize dynamic HDLC information between a Primary Route Processor (RP) and a Secondary RP.	<a href="#">Configuring Stateful Switchover</a>
	SSO - IGMP Snooping	This feature provides stateful switchover (SSO) support for Internet Group Management Protocol (IGMP) snooping. SSO with Layer 2 multicast state between the primary and the secondary supervisors. This feature allows the user to see virtually no interruption in multicast streams upon supervisor switchover.	<a href="#">Configuring Stateful Switchover</a>
	SSO - Multilink PPP (MLP)	This feature provides stateful switchover (SSO) support for Multilink Point-to-Point Protocol (PPP). With SSO, specific PPP state information is synchronized between the active Route Processor (RP) and standby RP. Single-link PPP and Multilink PPP (MLP) sessions are maintained during RP switchover for IP connections only.	<a href="#">Configuring Stateful Switchover</a>

**Table 1 Supported High Availability Features (continued)**

Release	Feature Name	Feature Description	Where Documented
Cisco IOS XE Release 2.1	SSO - PPP	This feature provides stateful switchover (SSO) support for Point-to-Point Protocol (PPP). With SSO, specific PPP state information is synchronized between the active Route Processor (RP) and standby RP.	<a href="#">Configuring Stateful Switchover</a>
	SSO - QoS	This feature provides stateful switchover (SSO) support for quality of service (QoS).	<a href="#">Configuring Stateful Switchover</a>
	Stateful Switchover	Development of the stateful switchover (SSO) feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS XE routers.	<a href="#">Configuring Stateful Switchover</a>
<b>Cisco IOS XE Release 2.3</b>			
Cisco IOS XE Release 2.3	ISSU - ATM	This feature provides In Service Software Upgrade (ISSU) support for ATM.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
	SSO - ATM	ATM Stateful Switchover (SSO) allows a router with redundant Route Processors (RPs) to exchange ATM state information to minimize the outage time due to RP failover.	<a href="#">Configuring Stateful Switchover</a>
<b>Cisco IOS XE Release 2.5</b>			
Cisco IOS XE Release 2.5	NSF/SSO - Multicast MPLS VPN	This feature is supported in Cisco IOS XE Release 2.5.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Nonstop Forwarding</a></li> <li>• <a href="#">Configuring Stateful Switchover</a></li> </ul>
	ISSU - Multicast MPLS VPN	This feature is supported in Cisco IOS XE Release 2.5.	<a href="#">Cisco IOS XE In Service Software Upgrade Process</a>
<b>Cisco IOS XE Release 3.1S</b>			
Cisco IOS XE 3.1S	ISSU - HSRPv6 on VRF interfaces	This feature provides ISSU - HSRPv6 on VRF interfaces for Cisco ASR 1000 Series Aggregation Services Routers.	<a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</a>
	NSF/SSO - HSRPv6 on VRF interfaces	This feature provides NSF/SSO support for HSRPv6 on VRF interfaces for Cisco ASR 1000 Series Aggregation Services Routers.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Nonstop Forwarding</a></li> <li>• <a href="#">Configuring Stateful Switchover</a></li> </ul>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1005R)

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

© 2007–2010 Cisco Systems, Inc. All rights reserved.





# Configuring Stateful Switchover

---

First Published: July 22, 2002

Last Updated: December 4, 2010

This document describes the Stateful Switchover (SSO) feature in Cisco IOS XE Software.

SSO provides a faster switchover relative to high system availability (HSA), and Router Processor Redundancy (RPR) by fully initializing and fully configuring the standby RP, and by synchronizing state information, which can reduce the time required for routing protocols to converge. Because SSO maintains stateful protocol and application information, user session information is maintained during a switchover, and line cards continue to forward network traffic with no loss of sessions, providing improved network availability. Network stability may be improved with the reduction in the number of route flaps had been created when routers in the network failed and lost their routing tables.

Throughout this document, the term “Route Processor” (RP) is used to describe the route processing engine.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Stateful Switchover” section on page 33](#).

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Stateful Switchover, page 2](#)
- [Restrictions for Stateful Switchover, page 2](#)
- [Information About Stateful Switchover, page 4](#)
- [How to Configure Stateful Switchover, page 19](#)



- [Configuration Examples for Configuring Stateful Switchover, page 29](#)
- [Additional References, page 31](#)
- [Feature Information for Stateful Switchover, page 33](#)

## Prerequisites for Stateful Switchover

- [General Prerequisites, page 2](#)
- [SNMP for Stateful Switchover Prerequisites, page 2](#)

### General Prerequisites

- For hardware redundant platforms, such as a Cisco ASR 1006 router, two RPs must be installed in the chassis, each running the same version or a compatible version of the Cisco IOS XE software.



**Note** For software redundant platforms, such as a Cisco ASR 1002 router or a Cisco ASR 1004 router, SSO mode is enabled in the configuration.

- 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).
```

### SNMP for Stateful Switchover Prerequisites

- The router must be in SSO mode.
- 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, page 3](#)
- [Switchover Process Restrictions, page 3](#)
- [ATM Restrictions, page 3](#)
- [Cisco ASR 1000 Series Aggregation Services Routers Restrictions, page 4](#)
- [SNMP for Stateful Switchover Restrictions, page 4](#)

## General Restrictions

- Both RPs must run the same Cisco IOS XE image. If the RPs are operating different Cisco IOS XE images, the system reverts to RPR mode even if SSO is configured. However, during the In Service Software Upgrade (ISSU) process, two RPs can run different Cisco IOS XE images as long as the images are ISSU-compatible.
- For Cisco NSF support, neighbor routers must be running Cisco NSF-enabled images, though SSO need not be configured on the neighbor device.
- Configuration changes made through SNMP may not be automatically configured on the standby RP after a switchover occurs.
- Load sharing between dual processors is not supported.
- For Cisco IOS XE Release 2.2, the following restrictions apply:
  - SSO is not supported for IP sessions or traffic class sessions.
  - SSO is not supported for any features on IP sessions or traffic class sessions.
  - SSO is not supported for the following features for PPP sessions: PBHK; L4RD; and Traffic class.
  - IP sessions are only present on the active router and are not checkpointed to the standby router. Therefore, upon switchover, sessions have to be reestablished and the subscriber must reselect services.

## 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:

```
Dec 3 04:05:55.350: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
Dec 3 04:05:55.418: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
```

## 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.

## ATM Restrictions

- The ATM line protocol does not support stateful switchover capability for the following features:
  - SVCs
  - Switched virtual paths (SVPs)
  - Tagged virtual circuits (TVCs)
  - Point-to-multipoint SVC
  - Integrated Local Management Interface (ILMI)
  - Signaling and Service Specific Connection Oriented Protocol (SSCOP)
  - ATM Connection Manager, PVC discovery, ATM applications

- Backward or version compatibility
- Statistics and accounting
- Zero ATM cell loss

## Cisco ASR 1000 Series Aggregation Services Routers Restrictions

- Only RPR and SSO are supported on the Cisco ASR 1000 Series Routers.
- RPR and SSO can be used on the Cisco ASR 1000 Series Router to enable a second Cisco IOS XE process on a single RP. This configuration option is only available on a Cisco ASR 1002 Router and Cisco ASR 1004 Router. On all other Cisco ASR 1000 Series Routers, the second Cisco IOS XE process can run on the standby RP only.
- A second IOS XE process can only be enabled using RPR or SSO if the RP is using 4 GB of DRAM. Use the **show version** command output to display the amount of DRAM configured on the router.

## 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 on page 17](#) 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, page 4](#)
- [Route Processor Redundancy Mode, page 7](#)
- [Stateful Switchover Mode, page 7](#)
- [Route Processor Synchronization, page 7](#)
- [Switchover Operation, page 9](#)
- [SSO-Aware Protocols and Applications, page 10](#)
- [Enhanced SNMP Support for High Availability, page 15](#)

## 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 key feature of the Cisco ASR 1000 Series Routers is that SSO can be used to enable a second Cisco IOS XE process on a single RP for software redundancy in the 2-RU and 4-RU chassis systems. These dual Cisco IOS XE packages can consist of the same software packages for backup or different packages for resilient upgrade. This second Cisco IOS XE process acts as a standby process for the active Cisco IOS XE process, and also allows certain subpackages to be upgraded without experiencing any router downtime.

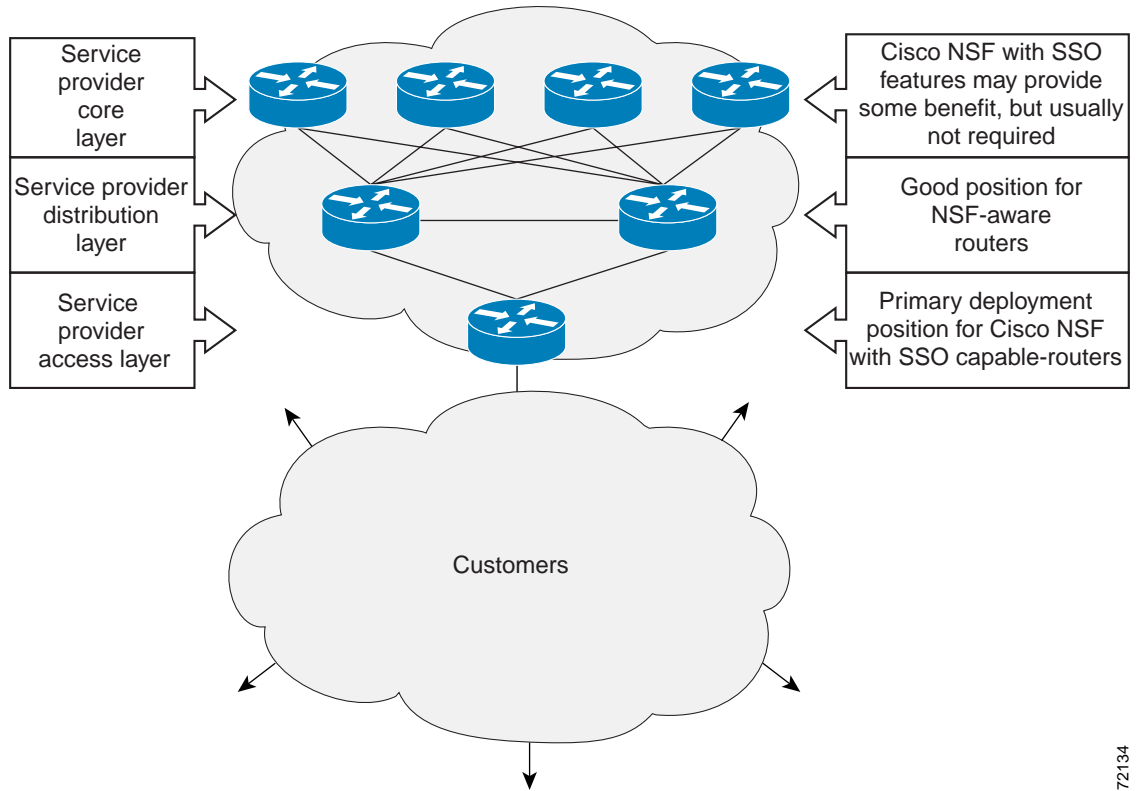
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

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.

[Figure 1](#) 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.

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.

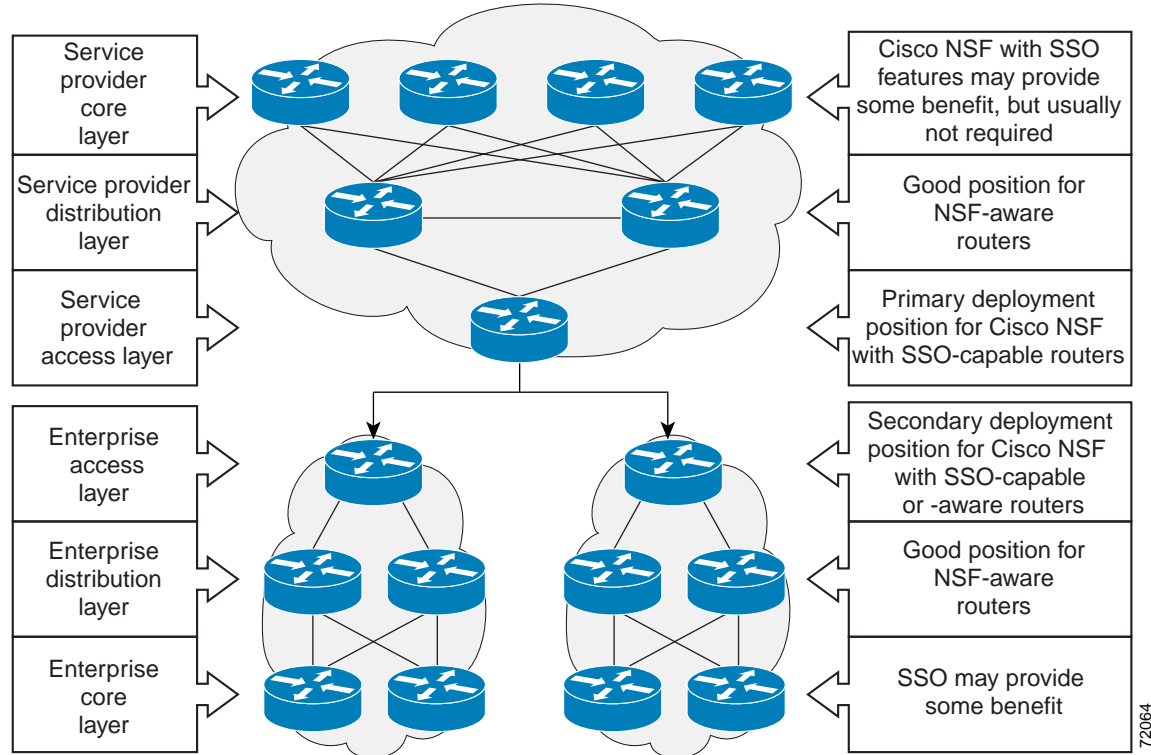
Figure 1 Cisco NSF with SSO Network Deployment: Service Provider Networks



72134

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. [Figure 2](#) 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



## Route Processor Redundancy Mode

Router Processor Redundancy (RPR) allows Cisco IOS XE Software to be booted on the standby processor prior to switchover (a “cold boot”). In RPR, the standby RP loads a Cisco IOS XE image at boot time and initializes itself in standby mode; however, although the startup configuration is synchronized to the standby RP, system changes are not. In the event of a fatal error on the active RP, the system switches to the standby processor, which reinitializes itself as the active processor, reads and parses the startup configuration, reloads all of the line cards, and restarts the system.

## Stateful Switchover Mode

SSO mode provides all the functionality of RPR+ in that the software is fully initialized on the standby RP. In addition, 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:

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

The synchronization of configuration information also applies to dual processes on a single RP.

## 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. For more information on SSO MIBs, see the “Additional References” section on page 31.

## Switchover Operation

- [Switchover Conditions, page 9](#)
- [Switchover Time, page 10](#)
- [Online Removal of the Active RP, page 10](#)
- [Core Dump Operation, page 10](#)

## 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 CLI 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 Cisco ASR 1000 Series Router. Packets that are switched or routed by the Cisco QuantumFlow Processor (QFP) on the switching fabric card 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.

The Cisco ASR 1000 Series Router has separate RPs and Forwarding Processor (FP). All transit packets are handles by the FP. Therefore, no transit packet loss occurs during RP switchover (dual RPs) or during IOSD process switchover (single RP).

## Online Removal of the Active RP

For Cisco ASR 1000 Series Routers that are configured to use SSO, online removal of the active RP automatically forces a stateful switchover to the standby RP.

## 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. For more information on how to complete a core dump, refer to the “Troubleshooting and Fault Management” chapter in the *Cisco IOS XE Network Management Configuration Guide*.



### 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 (such as PPP, Frame Relay, ATM, and SNMP) 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 (Frame Relay, ATM, and PPP) 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.

The following protocols and applications are SSO-aware:

- [Line Protocols, page 11](#)
- [Quality of Service, page 14](#)
- [IPv6 Support for Stateful Switchover, page 14](#)
- [Line Card Drivers, page 14](#)

## 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.

This section describes SSO supports for each of the line protocols described in the following sections:

- [ATM Stateful Switchover, page 11](#)
- [Frame Relay Stateful Switchover, page 12](#)
- [PPP and Multilink PPP Stateful Switchover, page 13](#)
- [HDLC Stateful Switchover, page 14](#)

## 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.



### Note

---

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

---

### 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.

#### ATM OAM Managed PVC or SVC Timeout

Operation, Administration, and Maintenance (OAM) F5 loopback cells must be echoed back on receipt by the remote host, thus demonstrating connectivity on the PVC between the router and the remote host. With ATM SSO, OAM loopback cells received on an interface must be echoed within 15 seconds before a PVC or switched virtual circuit (SVC) is declared down. By default, the OAM timeout is set to 10 seconds, followed by at most five retries sent at 1-second intervals. In the worst case, a switchover will begin just before expiration of the 10-second period, meaning that the PVC will go down within 5 seconds on the remote networking device if switchover has not completed within 5 seconds.



#### Note

---

Timers at remote ATM networking devices may be configurable, depending on the remote device owner.

---

## Frame Relay Stateful Switchover

With stateful switchover, Frame Relay 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).

#### Permanent Virtual Circuits

For Frame Relay to support forwarding during and after switchover, Frame Relay PVCs must remain up not only within the networking device, but also within the Frame Relay network.

In many cases the networking devices are connected to a switch, rather than back-to-back to another networking device, and that switch is not running Cisco IOS XE Software. The virtual circuit state is dependent on line state. PVCs are down when the line protocol is down. PVCs are up when the line protocol is up and the PVC status reported by the adjacent switch is active.

On point-to-point subinterfaces, or when static mappings are configured, Inverse ARP need not run. In cases where dynamic address mapping is used, an Inverse ARP protocol exchange determines the protocol address to data-link connection identifier (DLCI) mapping for the PVC. This exchange occurs as soon as the multipoint PVC makes the transition to active. If the exchange fails for some reason, for example, the remote networking device may drop the Inverse ARP request if it has not yet seen the PVC transition to active—any outstanding requests are run off a timer, with a default of 60 seconds.

#### Keepalive Messages

A crucial factor in maintaining PVCs is the delivery of Local Management Interface (LMI) protocol messages (keepalives) during switchover. This keepalive mechanism provides an exchange of information between the network server and the switch to verify that data is flowing.

If a number of consecutive LMI keepalives messages are lost or in error, the adjacent Frame Relay device declares the line protocol down and all PVCs on that interface are declared down within the Frame Relay network and reported as such to the remote networking device. The speed with which a switchover occurs is crucial to avoid the loss of keepalive messages.

The line protocol state depends on the Frame Relay keepalive configuration. With keepalives disabled, the line protocol is always up as long as the hardware interface is up. With keepalives enabled, LMI protocol messages are exchanged between the networking device and the adjacent Frame Relay switch. The line protocol is declared up after a number of consecutive successful LMI message exchanges.

The line protocol must be up according to both the networking device and the switch. The default number of exchanges to bring up the line protocol is implementation-dependent: Three is suggested by the standards; four is used on a Cisco Frame Relay switch, taking 40 seconds at the default interval of 10 seconds; and two is used on a Cisco IOS XE networking device acting as a switch or when connected back-to-back. This default number could be extended if the LMI “autosense” feature is being used while the LMI type expected on the switch is determined. The number of exchanges is configurable, although the switch and router may not have the same owner.

The default number of lost messages or errors needed to bring down the line is three (two on a Cisco IOS XE router). By default, if a loss of two messages is detected in 15 to 30 seconds, then a sequence number or LMI type error in the first message from the newly active RP takes the line down.

If a line goes down, consecutive successful LMI protocol exchanges (default of four over 40 seconds on a Cisco Frame Relay switch; default of two over 20 seconds on a Cisco IOS XE device) will bring the line back up again.

### 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.

---

## 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.

---

## 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 IOS XE 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.



Note

---

Distributed Cisco Express Forwarding must be enabled in order to run NSF.

---

## 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, page 16](#)
- [Network Management for SSO, page 16](#)
- [Uninterrupted Service Using SSO, page 16](#)
- [Communication with the NMS, page 17](#)
- [SSO MIB Support, page 17](#)
- [CISCO-RF-MIB Modifications for SSO Support, page 18](#)

## SNMP for Stateful Switchover Overview

The SNMP for Stateful Switchover MIBs feature provides support for managing a networking device running SSO. The MIB information provides the data for a network management application running the SNMP.

The SNMP and stateful switchover feature helps to improve the availability of networks made up of Cisco IOS XE-based 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 is based on the Internet Network Management Framework. This framework defines a model in which a managing system called a manager communicates with a managed system. The manager—typically referred to as the Network Management System, or NMS—runs a network management application, and the managed system runs an agent, which answers requests from the manager and generates notifications to the manager.

A MIB defines all the information about a managed system that a NMS can view or modify. The MIB is located on the managed system and can consist of standard and proprietary portions. The agent and manager each have their own view of the MIB. The NMS can be configured to periodically update its MIB view from all managed agents.

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

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, page 17](#)
- [Switchover Notification, page 17](#)
- [Traps, page 17](#)

### 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. For more information, see the “[CISCO-RF-MIB Modifications for SSO Support](#)” section.

### 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, page 18](#)
- [New Objects in CISCO-RF-MIB for SSO Support, page 19](#)

### 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, page 19](#)(required)
- [Setting the Configuration Register and Boot Variable, page 20](#) (required)
- [Setting the Configuration Register and Boot Variable, page 20](#) (required)
- [Configuring SSO, page 22](#) (required)
- [Configuring Frame Relay SSO for LMI Sequence Numbers Synchronization, page 23](#) (optional)
- [Verifying SSO Configuration, page 24](#) (optional)
- [Troubleshooting Stateful Switchover, page 24](#) (optional)

## Copying an Image onto an RP



### Note

To copy a consolidated package or subpackages onto active and standby RPs on the Cisco ASR 1000 Series Router, see the [Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide](#).

### SUMMARY STEPS

1. **enable**
2. **copy tftp bootflash:image**  
or  
**copy tftp harddisk:image**
3. **copy tftp stby-bootflash:image**  
or  
**copy tftp stby-harddisk:image**
4. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>copy tftp bootflash: <i>image</i></b> or <b>copy tftp harddisk: <i>image</i></b></p> <p><b>Example:</b> Router# copy tftp bootflash:asr1000rp1-adventerprisek9.02.01.00.1 22-33.XNA.bin or <b>Example:</b> Router# copy tftp harddisk:asr1000rp1-adventerprisek9.02.01.00.12 2-33.XNA.bin</p>	<p>Copies a Cisco IOS image using TFTP onto the flash device of the active RP.</p>
Step 3	<p><b>copy tftp stby-bootflash: <i>image</i></b> or <b>copy tftp stby-harddisk: <i>image</i></b></p> <p><b>Example:</b> Router# copy tftp stby-bootflash:asr1000rp1-adventerprisek9.02.01. .00.122-33.XNA.bin or <b>Example:</b> Router# copy tftp stby-harddisk:asr1000rp1-adventerprisek9.02.01. 00.122-33.XNA.bin</p>	<p>Copies a Cisco IOS image using TFTP onto the flash device of the standby RP.</p>
Step 4	<p><b>exit</b></p> <p><b>Example:</b> Router# exit</p>	<p>Exits to user EXEC mode.</p>

## Setting the Configuration Register and Boot Variable



## Note

Following the reload, each RP is in its default mode. SSO is the default mode for the Cisco ASR 1000 Series Routers. The default configuration register value is 0x102. However, on a reload, the system is booted with the last saved value.

### SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **no boot system flash** [*flash-fs:*][*partition-number:*][*filename*]  
or  
**no boot system tftp** *filename* [*ip-address*]
5. **boot system flash** [*flash-fs:*][*partition-number:*][*filename*]  
or  
**boot system tftp** *filename* [*ip-address*]
6. **config-register** *value*
7. **exit**
8. **copy running-config startup-config**
9. **reload**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show version</b>  <b>Example:</b> Router# show version	Obtains the current configuration register setting.
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>no boot system flash</b> [ <i>flash-fs:</i> ][ <i>partition-number:</i> ][ <i>filename</i> ] or <b>no boot system tftp</b> <i>filename</i> [ <i>ip-address</i> ]  <b>Example:</b> Router(config)# no boot system flash or  <b>Example:</b> Router(config)# no boot system ftp://192.0.7.19/cs3-rx.81-1	(Optional) Remove the startup system image specification.

	Command	Purpose
Step 5	<pre>boot system flash [flash-fs:] [partition-number:] [filename] or boot system tftp filename [ip-address]</pre> <p><b>Example:</b> Router(config)# boot system flash or</p> <p><b>Example:</b> Router(config)# boot system tftp://192.0.7.19/cs3-rx.83-2 </p>	Specifies the filename of image to be loaded at startup.
Step 6	<pre>config-register value</pre> <p><b>Example:</b> Router(config)# config-register 0x2102 </p>	(Optional) Modifies the existing configuration register setting to reflect the way in which you want to load a system image.
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit </p>	Exits to privileged EXEC mode.
Step 8	<pre>copy running-config startup-config</pre> <p><b>Example:</b> Router# copy running-config startup-config </p>	Saves the configuration changes to the startup configuration file.
Step 9	<pre>reload</pre> <p><b>Example:</b> Router# reload </p>	Reboots both RPs on the device to ensure that changes to the configuration take effect.

## Configuring SSO

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode {rpr | sso}**
5. **end**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  Example: Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<b>redundancy</b>  Example: Router(config)# redundancy	Enters redundancy configuration mode.
Step 4	<b>mode {rpr   sso}</b>  Example: Router(config-red)# mode sso	Sets the redundancy configuration mode to SSO on both the active and standby RP.  <b>Note</b> After configuring SSO mode, the standby RP will automatically reset.
Step 5	<b>end</b>  Example: Router(config-red)# end	Exits to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>  Example: Router# copy running-config startup-config	Saves the configuration changes to the startup configuration file.

## Configuring Frame Relay SSO for LMI Sequence Numbers Synchronization

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **frame-relay redundancy auto-sync lmi-sequence-numbers**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  Example: Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<b>frame-relay redundancy auto-sync lmi-sequence-numbers</b>  Example: Router(config)# frame-relay redundancy auto-sync lmi-sequence-numbers	Configures automatic synchronization of Frame Relay LMI sequence numbers between the active RP and the standby RP.

## Verifying SSO Configuration

## SUMMARY STEPS

1. **enable**
2. **show redundancy [clients | counters | history | switchover history | states]**
3. **show redundancy states**

## DETAILED STEPS

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

## Troubleshooting Stateful Switchover

- [Possible SSO Problem Situations, page 25](#)

- [Troubleshooting SSO, page 25](#)
- [Troubleshooting SNMP for Stateful Switchover, page 28](#)

## Possible SSO Problem Situations

This section describes possible situations in which SSO troubleshooting may be needed.

- 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:

```
Router# show redundancy history
```

- 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.

During the upgrade process, different images will be loaded on the RPs for a short period of time. If a switchover occurs during this time, the device will recover in RPR mode.

- 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 ISSU procedure is complete, each RP will be running a different software version. While the RPs are running different software versions, the mode will change to RPR. The device will change to SSO mode once the upgrade has completed. For more information on ISSU, see the “[In Service Software Upgrade](#)” module in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.

- In Cisco IOS XE Software, 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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **crashdump-timeout** [*mm* | *hh:mm*]

5. **end**
6. **debug atm ha-error**
7. **debug atm ha-events**
8. **debug atm ha-state**
9. **debug frame-relay redundancy**
10. **debug ppp redundancy [detailed | event]**
11. **debug redundancy {config-sync | ehfa | errors | fsm | ldb-sync-history | kpa | msg | progression | status | timer}**
12. **show diag [slot-number / chassis | subslot slot/subslot] [details | summary]**
13. **show redundancy [clients | counters | history | switchover history | states]**
14. **show version**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  Example: Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<b>redundancy</b>  Example: Router(config)# redundancy	Enters redundancy configuration mode.
Step 4	<b>crashdump-timeout</b> [mm   hh:mm]  Example: router(config-red)# crashdump-timeout	Set the longest time that the newly active RSP will wait before reloading the formerly active RSP.
Step 5	<b>end</b>  Example: Router(config-red)# exit	Exits to privileged EXEC mode.
Step 6	<b>debug atm ha-error</b>  Example: Router# debug atm ha-error	Displays information about ATM HA errors on the networking device.
Step 7	<b>debug atm ha-events</b>  Example: Router# debug atm ha-events	Displays information about ATM HA events on the networking device.
Step 8	<b>debug atm ha-state</b>  Example: Router# debug atm ha-state	Displays information about ATM high-availability state information on the networking device.
Step 9	<b>debug frame-relay redundancy</b>  Example: Router# debug frame-relay redundancy	Displays information about Frame Relay redundancy on the networking device.
Step 10	<b>debug ppp redundancy</b> [detailed   event]  Example: Router# debug ppp redundancy	Displays information about PPP redundancy on the networking device.

	Command	Purpose
Step 11	<pre>debug redundancy {config-sync   ehpa   errors   fsm   ldb-sync-history   kpa   msg   progression   status   timer}</pre> <p><b>Example:</b> Router# debug redundancy all</p>	Displays information about redundancy on the networking device.
Step 12	<pre>show diag [slot-number   chassis   subslot slot/subslot] [details   summary]</pre> <p><b>Example:</b> Router# show diag</p>	Displays hardware information for the router.
Step 13	<pre>show redundancy [clients   counters   history   switchover history   states]</pre> <p><b>Example:</b> Router# show redundancy</p>	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 14	<pre>show version</pre> <p><b>Example:</b> Router# show version</p>	Displays image information for each RP.

## Troubleshooting SNMP for Stateful Switchover

### SUMMARY STEPS

1. **enable**
2. **show redundancy history**
3. **show redundancy switchover history**
4. **debug snmp sync**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>show redundancy history</pre> <p><b>Example:</b> Router# show redundancy history</p>	Displays switchover history.

	Command or Action	Purpose
Step 3	<b>show redundancy switchover history</b>  <b>Example:</b> Router# show redundancy switchover history	Displays switchover history details.
Step 4	<b>debug snmp sync</b>  <b>Example:</b> Router# debug snmp sync	Displays information about SNMP synchronization and faults in synchronization.
Step 5	<b>exit</b>  <b>Example:</b> Router# exit	Exits to user EXEC mode.

## Configuration Examples for Configuring Stateful Switchover

- [Example: SSO on the Cisco ASR 1000 Series Router, page 29](#)
- [Example: SSO Protocols and Applications Registered on the Cisco ASR Series Router, page 29](#)

### Example: SSO on the Cisco ASR 1000 Series Router

The following sample output shows that SSO is configured on the Cisco ASR 1000 Series Router:

```
Router# show redundancy states

    my state = 13 -ACTIVE
    peer state = 8 -STANDBY HOT
        Mode = Duplex
        Unit ID = 49

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

    client count = 67
    client_notification_TMR = 30000 milliseconds
    RF debug mask = 0x0
```

### Example: SSO Protocols and Applications Registered on the Cisco ASR Series Router

The following sample output shows a list of applications and protocols that have registered as SSO protocols or applications on the Cisco ASR 1000 Series Router:

Router# **show redundancy clients**

```

clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 29     clientSeq = 60     Redundancy Mode RF
clientID = 139    clientSeq = 62     IfIndex
clientID = 25     clientSeq = 69     CHKPT RF
clientID = 1340   clientSeq = 90     ASR1000-RP Platform
clientID = 1501   clientSeq = 91     Cat6k CWAN HA
clientID = 78     clientSeq = 95     TSPTUN HA
clientID = 305    clientSeq = 96     Multicast ISSU Conso
clientID = 304    clientSeq = 97     IP multicast RF Clie
clientID = 22     clientSeq = 98     Network RF Client
clientID = 88     clientSeq = 99     HSRP
clientID = 114    clientSeq = 100    GLBP
clientID = 1341   clientSeq = 102    ASR1000 DPIDX
clientID = 1505   clientSeq = 103    Cat6k SPA TSM
clientID = 1344   clientSeq = 110    ASR1000-RP SBC RF
clientID = 227    clientSeq = 111    SBC RF
clientID = 71     clientSeq = 112    XDR RRP RF Client
clientID = 24     clientSeq = 113    CEF RRP RF Client
clientID = 146    clientSeq = 114    BFD RF Client
clientID = 306    clientSeq = 120    MFIB RRP RF Client
clientID = 1504   clientSeq = 128    Cat6k CWAN Interface
clientID = 75     clientSeq = 130    Tableid HA
clientID = 401    clientSeq = 131    NAT HA
clientID = 402    clientSeq = 132    TPM RF client
clientID = 5      clientSeq = 135    Config Sync RF clien
clientID = 68     clientSeq = 149    Virtual Template RF
clientID = 23     clientSeq = 152    Frame Relay
clientID = 49     clientSeq = 153    HDLC
clientID = 72     clientSeq = 154    LSD HA Proc
clientID = 113    clientSeq = 155    MFI STATIC HA Proc
clientID = 20     clientSeq = 171    IPROUTING NSF RF cli
clientID = 100    clientSeq = 173    DHCPC
clientID = 101    clientSeq = 174    DHCPD
clientID = 74     clientSeq = 183    MPLS VPN HA Client
clientID = 34     clientSeq = 185    SNMP RF Client
clientID = 52     clientSeq = 186    ATM
clientID = 69     clientSeq = 189    AAA
clientID = 118    clientSeq = 190    L2TP
clientID = 82     clientSeq = 191    CCM RF
clientID = 35     clientSeq = 192    History RF Client
clientID = 90     clientSeq = 204    RSVP HA Services
clientID = 70     clientSeq = 215    FH COMMON RF CLIENT
clientID = 54     clientSeq = 220    SNMP HA RF Client
clientID = 73     clientSeq = 221    LDP HA
clientID = 76     clientSeq = 222    IPRM
clientID = 57     clientSeq = 223    ARP
clientID = 50     clientSeq = 230    FH_RF_Event_Detector
clientID = 1342   clientSeq = 240    ASR1000 SpaFlow
clientID = 1343   clientSeq = 241    ASR1000 IF Flow
clientID = 83     clientSeq = 255    AC RF Client
clientID = 84     clientSeq = 257    AToM manager
clientID = 85     clientSeq = 258    SSM
clientID = 102    clientSeq = 273    MQC QoS
clientID = 94     clientSeq = 280    Config Verify RF cli
clientID = 135    clientSeq = 289    IKE RF Client
clientID = 136    clientSeq = 290    IPSEC RF Client
clientID = 130    clientSeq = 291    CRYPTO RSA
clientID = 148    clientSeq = 296    DHCPv6 Relay
clientID = 4000   clientSeq = 303    RF_TS_CLIENT
clientID = 4005   clientSeq = 305    ISSU Test Client
clientID = 93     clientSeq = 309    Network RF 2 Client
clientID = 205    clientSeq = 311    FEC Client

```

```

clientID = 141      clientSeq = 319      DATA_DESCRIPTOR RF C
clientID = 4006    clientSeq = 322      Network Clock
clientID = 225     clientSeq = 326      VRRP
clientID = 65000   clientSeq = 336      RF_LAST_CLIENT

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS High Availability commands	<a href="#">Cisco IOS High Availability Command Reference</a>
Cisco IOS debug commands	<a href="#">Cisco IOS Debug Command Reference</a>
Cisco nonstop forwarding	<a href="#">Configuring Nonstop Forwarding</a>
DHCP proxy client	“ISSU and SSO--DHCP High Availability Features,” module of the <a href="#">Cisco IOS XE IP Addressing Services Configuration Guide</a> .
SSO - BFD	“Bidirectional Forwarding Detection” chapter in the <a href="#">Cisco IOS XE IP Routing Protocols</a>
SSO HSRP	“Configuring HSRP” chapter in the <a href="#">Cisco IOS XE IP Application Services Configuration Guide</a>
SSO - MPLS VPN 6VPE and 6PE SSO support	<a href="#">NSF/SSO and ISSU - MPLS VPN 6VPE and 6PE</a>
SSO and RPR on the Cisco ASR 1000 Series Routers	<a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</a>
SSO VRRP	“Configuring VRRP” chapter in the <a href="#">Cisco IOS IP XE Application Services Configuration Guide</a>
Basic IPv6 configuration	“Implementing IPv6 Addressing and Basic Connectivity” chapter in the <a href="#">Cisco IOS XE IPv6 Configuration Guide</a>
SNMP configuration tasks	“Configuring SNMP Support” module of <a href="#">Cisco IOS XE Network Management Configuration Guide</a>
SNMP commands	<a href="#">Cisco IOS Network Management Command Reference</a>

### Standards

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

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>CISCO-RF-MIB—This MIB has been modified for SNMP for SSO.</li> <li>ENTITY-MIB</li> <li>IF-MIB</li> <li>SNMP-FRAMEWORK-MIB</li> <li>SNMP-TARGET-MIB</li> <li>SNMP-USM-MIB</li> <li>SNMP-VACM-MIB</li> <li>SNMPv2-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS Software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 1907	<i>Management Information Base for Version 2 of the Simple Network Management Protocol</i>
RFC 2571	<i>An Architecture for Describing SNMP Management Frameworks</i>
RFC 2573	<i>SNMP Applications</i>
RFC 2574	<i>User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)</i>
RFC 2575	<i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>
RFC 2863	<i>The Interfaces Group MIB</i>
RFC 4133	<i>Entity MIB (Version 3)</i>

## Technical Assistance

Description	Link
<p>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.</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

# Feature Information for Stateful Switchover

**Table 1** lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

**Table 1** lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 1** Feature Information for Cisco Stateful Switchover

Feature Name	Releases	Feature Information
Stateful Switchover (SSO)	Cisco IOS XE Release 2.1	<p>The following features were introduced:</p> <ul style="list-style-type: none"> <li>• Dual IOS processes on the same RP was introduced.</li> <li>• IPv6: Base protocols high availability</li> <li>• NSF/SSO (Nonstop Forwarding with Stateful Switchover) <ul style="list-style-type: none"> <li>– NSF/SSO - HSRPv6</li> <li>– NSF/SSO - IPsec</li> <li>– NSF/SSO - IPv6 uRPF</li> <li>– NSF/SSO - Managed LNS MPLS</li> <li>– NSF/SSO - MLD Access Group</li> <li>– NSF/SSO - MPLS VPN</li> <li>– NSF/SSO - VRRP</li> </ul> </li> <li>• Stateful Switchover (SSO) <ul style="list-style-type: none"> <li>– SSO - Frame Relay</li> <li>– SSO - HDLC</li> <li>– SSO - IGMP Snooping</li> <li>– SSO - Multilink PPP (MLP)</li> <li>– SSO - PPP</li> <li>– SSO - QoS</li> </ul> </li> </ul> <p>The following commands were introduced or modified: <b>crashdump-timeout</b>, <b>debug frame-relay redundancy</b>, <b>debug ppp redundancy</b>, <b>debug qos ha</b>, <b>debug redundancy</b>, <b>frame-relay redundancy auto-sync</b>, <b>lmi-sequence-numbers</b>, <b>mode (redundancy)</b>, <b>redundancy</b>, <b>redundancy force-switchover</b>, <b>reload</b>, <b>show redundancy</b>.</p>

Table 1 Feature Information for Cisco Stateful Switchover (continued)

Feature Name	Releases	Feature Information
Enhanced SNMP Support for High Availability	Cisco IOS XE Release 2.1	The Enhanced SNMP Support for High Availability feature provides support for managing a networking device running stateful switchover (SSO).  The following commands were introduced or modified: <b>debug snmp sync, show isis nfs, show redundancy.</b>
NSF/SSO - HSRPv6 on VRF interfaces	Cisco IOS XE Release 3.1S	This feature was introduced for Cisco ASR 1000 Series Aggregation Services Routers was introduced.
NSF/SSO - Multicast MPLS VPN	Cisco IOS XE Release 2.5	This feature was introduced.
SSO - ATM	Cisco IOS XE Release 2.3	This feature was introduced.  The following commands were introduced or modified: <b>debug atm ha-error, debug atm ha-events, debug atm ha-state.</b>
SSO - BFD	Cisco IOS XE Release 2.5	This feature was introduced.
SSO - MPLS VPN 6VPE and 6PE SSO support	Cisco IOS XE Release 2.5	This feature was introduced.
SSO - PPPoE IPv6	Cisco IOS XE Release 2.5	This feature was introduced.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1005R)

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

© 2002–2010 Cisco Systems, Inc. All rights reserved.



# Configuring Nonstop Forwarding

---

**First Published:** July 22, 2002

**Last Updated:** November 22, 2010

Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) feature in Cisco IOS XE 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.

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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Configuring Nonstop Forwarding”](#) section on page 24.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Configuring Nonstop Forwarding, page 2](#)
- [Restrictions for Configuring Nonstop Forwarding, page 2](#)
- [Information About Configuring Nonstop Forwarding, page 3](#)
- [How to Configure Nonstop Forwarding, page 9](#)
- [Configuration Examples for Configuring Nonstop Forwarding, page 18](#)
- [Additional References, page 22](#)



---

Americas Headquarters:

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

- [Feature Information for Configuring Nonstop Forwarding, page 24](#)

## Prerequisites for Configuring Nonstop Forwarding

- The networking device that is to be configured for NSF must first be configured for SSO. For information, see [Stateful Switchover](#).
- 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 Configuring Nonstop Forwarding

- [General Restrictions, page 2](#)
- [BGP NSF Restrictions, page 2](#)
- [EIGRP NSF Restrictions, page 3](#)
- [OSPF NSF Restrictions, page 3](#)

### General Restrictions

- The Hot Standby Routing Protocol (HSRP) is not supported with Cisco NSF with SSO. Do not use HSRP with Cisco NSF with SSO.

### 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 IOS XE 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 IOS XE 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.
- 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 Configuring Nonstop Forwarding

- [Nonstop Forwarding, page 3](#)
- [Cisco SSO, page 4](#)
- [Cisco NSF Routing and Forwarding, page 5](#)
- [Cisco Express Forwarding and NSF, page 5](#)
- [BGP NSF Operations, page 6](#)
- [EIGRP NSF Operations, page 6](#)
- [IPv6 support for NSF Operations, page 7](#)
- [IS-IS NSF Operations, page 8](#)
- [OSPF NSF Operations, page 9](#)

## Nonstop Forwarding



Note

---

Throughout this document, 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 IOS XE 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).
- Prevents 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.

## Cisco SSO

NSF always runs together with SSO. In specific Cisco networking devices that support dual RPs, SSO establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizes 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.

In networking devices running SSO, both RPs must be running the same configuration so that the standby RP is always ready to assume control following a fault on the active RP. The configuration information is synchronized from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. Following an initial synchronization between the two processors, SSO maintains RP state information between them, including forwarding information.

During switchover, system control and routing protocol execution is transferred from the active processor to the standby processor. The time required by the device to switch over from the active to the standby processor ranges from just a few seconds to approximately 30 seconds, depending on the platform.

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 through an RP switchover. For some HA-aware protocols and applications, state information is synchronized from the active to the standby processor. For Cisco NSF, enhancements to the routing protocols (CEF; OSPF; BGP; and IS-IS) have been made to support the HA features in SSO.

## 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

EIGRP 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 -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

The following sections provide information about IPv6 support for NSF for specific features:

- [Nonstop Forwarding and Graceful Restart for MP-BGP IPv6 Address Family, page 7](#)
- [Nonstop Forwarding for IPv6 RIP, page 7](#)
- [Nonstop Forwarding for Static Routes, page 8](#)

## 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 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.

For information about how to configure the IPv6 BGP graceful restart capability, see [Implementing Multiprotocol BGP for IPv6](#).

## 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 supports IETF IS-IS and Cisco IS-IS for configuring NSF. For information, see the following sections:

- [IETF IS-IS Configuration, page 8](#)
- [Cisco IS-IS Configuration, page 9](#)

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 abort 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.

## OSPF NSF Operations

Before an OSPF NSF-capable device can perform an RP switchover, it must relearn the available OSPF neighbors on the network, without resetting the neighbor relationship, and it must reacquire the contents of the Link State Database for the network.

To do this, 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. Then the NSF-capable device uses the signals it receives from other devices on the network to rebuild its neighbor list.

Next, the NSF-capable device resynchronizes its database with all of the NSF-aware neighbors on its list. After all of the neighbors exchange routing information, the NSF-capable device uses the routing information to remove stale routes, update the RIB, and update the 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 NSF device modes of operation common to the Cisco and IETF NSF implementations are as follows:

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

The strict LSA checking feature allows a helper device to terminate the graceful restart process if it 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, page 10](#) (optional)

- [Configuring and Verifying EIGRP NSF, page 11](#) (optional)
- [Configuring OSPF NSF, page 12](#) (optional)
- [Configuring and Verifying IS-IS NSF, page 15](#) (optional)
- [Troubleshooting Nonstop Forwarding, page 16](#) (optional)

## Configuring and Verifying BGP NSF

Repeat this task on each peer device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*]
5. **end**
6. **show ip bgp neighbors** [*ip-address* | **advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy** [**detail**]]

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  Example: Router(config)# router bgp 120	Enables a BGP routing process, and enters router configuration mode.
Step 4	<b>bgp graceful-restart</b> [ <b>restart-time</b> <i>seconds</i>   <b>stalepath-time</b> <i>seconds</i> ]  Example: Router(config-router)# bgp graceful-restart	Enables the BGP graceful restart capability, which starts NSF for BGP.

	Command	Purpose
Step 5	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits to privileged EXEC mode.
Step 6	<b>show ip bgp neighbors</b> [ <i>ip-address</i> [ <b>advertised-routes</b>   <b>dampened-routes</b>   <b>flap-statistics</b>   <b>paths</b> [ <i>reg-exp</i> ]   <b>received prefix-filter</b>   <b>received-routes</b>   <b>routes</b>   <b>policy</b> [ <b>detail</b> ]]]  <b>Example:</b> Router# show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

## Configuring and Verifying EIGRP NSF

Repeat this task on each peer device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **no nsf**
5. **timers nsf converge** *seconds*
6. **timers nsf signal** *seconds*
7. **timers graceful-restart purge-time** *seconds*
8. **end**
9. **show ip protocols**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router eigrp 109	Enables an EIGRP routing process, and enters router configuration mode.

	Command	Purpose
Step 4	<b>nsf</b>  Example: Router(config)# no nsf	(Optional) Enables NSF capabilities. <ul style="list-style-type: none"> <li>This command is enabled by default.</li> </ul>
Step 5	<b>timers nsf converge</b> <i>seconds</i>  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. <ul style="list-style-type: none"> <li>Enter this command on NSF-capable devices only.</li> </ul>
Step 6	<b>timers nsf signal</b> <i>seconds</i>  Example: Router(config-router)# timers nsf signal 20	(Optional) Adjusts the maximum time for the initial restart period. <ul style="list-style-type: none"> <li>Enter this command on NSF-capable devices only.</li> </ul>
Step 7	<b>timers graceful-restart purge-time</b> <i>seconds</i>  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. <ul style="list-style-type: none"> <li>This command is supported in Cisco IOS Release 12.2(33)SRE and later releases.</li> </ul>
Step 8	<b>end</b>  Example: Router(config-router)# end	Exits to privileged EXEC mode.
Step 9	<b>show ip protocols</b>  Example: Router# show ip protocols	Displays the parameters and current state of the active routing protocol process.

## Configuring OSPF NSF

Perform only one of the following tasks to configure OSPF NSF:

- [Configuring Cisco NSF for OSPF, page 12](#)
- [Configuring IETF NSF for OSPF, page 13](#)

## Configuring Cisco NSF for OSPF

Perform this task to configure Cisco NSF support for OSPF on your all-Cisco network.

### SUMMARY STEPS

- enable**
- configure terminal**
- router ospf** *process-id* [**vrf** *vpn-name*]
- nsf cisco** [**enforce-global**]

5. **no nsf cisco helper disable**
6. **nsf ietf helper disable**
7. **end**
8. **show ip ospf nsf**

**DETAILED STEPS**

	<b>Command</b>	<b>Purpose</b>
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router ospf process-id [vrf vpn-name]</b>  <b>Example:</b> Router(config)# router ospf 12	Enables OSPF and enters router configuration mode.
Step 4	<b>nsf cisco [enforce global]</b>  <b>Example:</b> Router(config-router)# nsf cisco	Enables Cisco NSF restarting mode. <ul style="list-style-type: none"><li>• This command is not required on devices that will operate in NSF helper mode only.</li></ul>
Step 5	<b>no nsf cisco helper disable</b>  <b>Example:</b> Router(config-router)# no nsf cisco helper disable	(Optional) Reenables Cisco NFS helper support. <ul style="list-style-type: none"><li>• This command is included here only to show how to reenables Cisco NSF helper mode if helper mode was explicitly disabled</li></ul>
Step 6	<b>nsf ietf helper disable</b>  <b>Example:</b> Router(config-router)# nsf ietf helper disable	(Optional) Disables IETF NSF helper mode on an NSF-aware device.
Step 7	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits to privileged EXEC mode.
Step 8	<b>show ip ospf nsf</b>  <b>Example:</b> Router# show ip ospf nsf	Displays OSPF NSF state information

**Configuring IETF NSF for OSPF**

Perform this task to configure Cisco IETF NSF support for OSPF on your multivendor network.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf ietf** [**restart-interval** *seconds*]
5. **nsf ietf** [**helper** [**disable** | **strict-lsa-checking**]]
6. **no nsf ietf helper disable**
7. **nsf cisco helper disable**
8. **end**
9. **show ip ospf nsf**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vpn-name</i> ]  Example: Router(config)# router ospf 12	Enables OSPF and enters router configuration mode.
Step 4	<b>nsf ietf</b> [ <b>restart-interval</b> <i>seconds</i> ]  Example: Router(config-router)# nsf ietf restart-interval 180	Enables IETF NSF restarting mode. <ul style="list-style-type: none"> <li>• This command is not required on devices that will operate in helper mode only.</li> </ul>
Step 5	<b>nsf ietf</b> [ <b>helper</b> [ <b>disable</b>   <b>strict-lsa-checking</b> ]]  Example: Router(config-router)# nsf ietf helper strict-lsa-checking	(Optional) Configures IETF NSF helper mode on neighbor devices that will operate in helper mode.
Step 6	<b>no nsf ietf helper disable</b>  Example: Router(config-router)# no nsf ietf helper disable	(Optional) Reenables IETF NSF helper mode. <ul style="list-style-type: none"> <li>• This command is included here only to show how to reenables IETF NSF helper mode if helper mode was explicitly disabled.</li> </ul>
Step 7	<b>nsf cisco helper disable</b>  Example: Router(config-router)# nsf cisco helper disable	(Optional) Disables Cisco NSF helper mode on an NSF-aware device.

	Command	Purpose
Step 8	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits to privileged EXEC mode.
Step 9	<b>show ip ospf nsf</b>  <b>Example:</b> Router# show ip ospf nsf	Displays OSPF NSF state information

## Configuring and Verifying IS-IS NSF

### SUMMARY STEPS

1. **enable**
  2. **configure terminal**
  3. **router isis** *area-tag*
  4. **nsf** [**cisco** | **ietf**]
  5. **nsf interval** *minutes*
- For IETF NSF only:
6. **nsf t3** {**manual** *seconds* | **adjacency**}
- For Cisco NSF only:
7. **nsf interface wait** *seconds*
  8. **end**
  9. **show isis nsf**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router isis</b> <i>area-tag</i>  <b>Example:</b> Router(config)# router isis cisco1	Enables the IS-IS routing protocol to specify an IS-IS process and enters router configuration mode.

	Command	Purpose
Step 4	<b>nsf</b> [ <b>cisco</b>   <b>ietf</b> ]  <b>Example:</b> Router(config-router)# nsf ietf	Enables IS-IS NSF operations.
Step 5	<b>nsf interval</b> <i>minutes</i>  <b>Example:</b> Router(config-router)# nsf interval 2	(Optional) Configures the minimum time between NSF restart attempts.
Step 6	<b>nsf t3</b> { <b>manual</b> <i>seconds</i>   <b>adjacency</b> }  <b>Example:</b> 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.  <ul style="list-style-type: none"> <li>This command is supported for IETF NSF only.</li> </ul>
Step 7	<b>nsf interface wait</b> <i>seconds</i>  <b>Example:</b> 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.  <ul style="list-style-type: none"> <li>This command is supported for Cisco NSF only.</li> </ul>
Step 8	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits to privileged EXEC mode.
Step 9	<b>show isis nsf</b>  <b>Example:</b> Router# show isis nsf	Displays current state information regarding IS-IS NSF.

## Troubleshooting Nonstop Forwarding

### SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug ip eigrp notifications**
4. **debug isis nsf [detail]**
5. **debug ospf nsf [detail]**
6. **show cef nsf**
7. **show cef state**
8. **show clns neighbors**
9. **show ip bgp**

10. **show ip bgp neighbor**
11. **show ip cef**
12. **show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**]
13. **show ip ospf**
14. **show ip ospf neighbor** [**detail**]
15. **show ip protocols**
16. **show isis database** [**detail**]
17. **show isis nsf**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug eigrp nsf</b>  <b>Example:</b> Router# debug eigrp nsf	Displays notifications and information about NSF events for an EIGRP routing process.
Step 3	<b>debug ip eigrp notifications</b>  <b>Example:</b> Router# debug ip eigrp notifications	Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.
Step 4	<b>debug isis nsf [detail]</b>  <b>Example:</b> Router# debug isis nsf [detail]	Displays information about the IS-IS state during a Cisco NSF restart.
Step 5	<b>debug ospf nsf [detail]</b>  <b>Example:</b> Router# debug ospf nsf [detail]	Displays debugging messages related to OSPF Cisco NSF commands.
Step 6	<b>show cef nsf</b>  <b>Example:</b> Router# show cef nsf	Displays the current NSF state of CEF on both the active and standby RPs.
Step 7	<b>show cef state</b>  <b>Example:</b> Router# show cef state	Displays the CEF state on a networking device.
Step 8	<b>show clns neighbors</b>  <b>Example:</b> Router# show clns neighbors	Display both end system and intermediate system neighbors.

	Command	Purpose
Step 9	<b>show ip bgp</b>  Example: Router# show ip bgp	Displays entries in the BGP routing table.
Step 10	<b>show ip bgp neighbor</b>  Example: Router# show ip bgp neighbor	Displays information about the TCP and BGP connections to neighbor devices.
Step 11	<b>show ip cef</b>  Example: Router# show ip cef	Displays entries in the FIB that are unresolved, or displays a FIB summary.
Step 12	<b>show ip eigrp neighbors</b> [ <i>interface-type</i>   <i>as-number</i>   <b>static</b>   <b>detail</b> ]  Example: Router# show ip eigrp neighbors detail	To display detailed information about neighbors discovered by EIGRP.
Step 13	<b>show ip ospf</b>  Example: Router# show ip ospf	Displays general information about OSPF routing processes.
Step 14	<b>show ip ospf neighbor</b> [ <b>detail</b> ]  Example: Router# show ip ospf neighbor [detail]	Displays OSPF-neighbor information on a per-interface basis.
Step 15	<b>show ip protocols</b>  Example: Router# show ip protocols	Displays the parameters and current state of the active routing protocol process. <ul style="list-style-type: none"> <li>The status of EIGRP NSF configuration and support is displayed in the output.</li> </ul>
Step 16	<b>show isis database</b> [ <b>detail</b> ]  Example: Router# show isis database [detail]	Displays the IS-IS link-state database.
Step 17	<b>show isis nsf</b>  Example: Router# show isis nsf	Displays the current state information regarding IS-IS NSF.

## Configuration Examples for Configuring Nonstop Forwarding

- [Example: NSF-Capable CEF, page 19](#)
- [Example: BGP NSF, page 19](#)
- [Example: EIGRP NSF, page 20](#)

- [Example: OSPF and Cisco NSF, page 20](#)
- [Example: OSPF and IETF NSF, page 21](#)
- [Example: IS-IS NSF, page 21](#)

## Example: NSF-Capable CEF

The CEF NSF feature operates by default while the networking device 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]

CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
CEF default capabilities:
Always FIB switching:      yes
Default CEF switching:    yes
Default dCEF switching:   yes
Update HWIDB counters:    no
Drop multicast packets:   no
CEF NSF capable:       yes
IPC delayed func on SSO:  no
RRP state:
I am standby RRP:         no
My logical slot:          0
RF PeerComm:              no
```

## 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 displays the default or user-defined value for the route-hold timer.
- “EIGRP NSF enabled,” or “EIGRP NSF disabled,” appears in the output only when the NSF capability is supported by the device.

```
Router# 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: OSPF and Cisco NSF

The following output from the **show ip ospf nsf** command shows that NSF is enabled for OSPF process 400. NSF helper mode is enabled by default on routers running NSF-compatible software. Note that in this configuration, IETF helper mode is disabled for process 400.

```
Router> 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 192.0.2.155, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

## Example: OSPF and IETF NSF

The following output from the **show ip ospf nsf** command shows that NSF is enabled for OSPF process 500. NSF helper mode is enabled by default on routers running NSF-compatible software. Note that in this configuration, Cisco helper mode is disabled.

```
Router> 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 192.0.2.2, 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-IS NSF

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 will be different on the active and standby RPs.

The following sample output for the Cisco configuration on the active RP shows that NSF is enabled on the device (NSF restart enabled):

```
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 for the Cisco configuration 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 commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco debug commands	<a href="#">Cisco IOS DEbug Command Reference</a>
Cisco IOS high Availability commands	<a href="#">Cisco IOS High Availability Command Reference</a>
BGP support for NSF/SSO	<a href="#">BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)</a>
EIGRP nonstop forwarding awareness	<a href="#">EIGRP Nonstop Awareness</a>
IPv6 BGP Graceful Restart	<a href="#">“Implementing Multiprotocol BGP for IPv6,” Cisco IOS XE IPv6 Configuration Guide</a>
IPv6 RIP	<a href="#">“Implementing RIP for IPv6,” Cisco IOS XE IPv6 Configuration Guide</a>

Related Topic	Document Title
IPv6 static routes	<a href="#">“Implementing Static Routes for IPv6,”</a> <i>Cisco IOS XE IPv6 Configuration Guide</i>
NSF/SSO—MPLS VPN	<a href="#">“Configuring NSF/SSO—MPLS VPN”</a> module in the <i>MPLS Configuration Guide</i>
Stateful switchover	<a href="#">“Stateful Switchover,”</a> <i>Cisco IOS XE High Availability Configuration Guide</i>

## Standards

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

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 3623	<i>Graceful OSPF Restart</i>
RFC 3847	<i>Restart Signaling for Intermediate System to Intermediate System (IS-IS)</i>
RFC 4781	<i>Graceful Restart Mechanism for BGP</i>

## 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for Configuring Nonstop Forwarding

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


**Note**

Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 1** Feature Information for Cisco Nonstop Forwarding

Feature Name	Releases	Feature Information
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	Cisco IOS XE Release 2.1	<p>The following features were introduced:</p> <ul style="list-style-type: none"> <li>• IPv6: Static route nonstop forwarding</li> <li>• IPv6: RIPng nonstop forwarding</li> <li>• IPv6: NSF and graceful restart for MP-BGP IPv6 address family</li> <li>• IPv6: Base protocols high availability</li> <li>• NSF Awareness (Nonstop Forwarding Awareness) <ul style="list-style-type: none"> <li>– NSF - BGP</li> <li>– NSF - EIGRP</li> <li>– NSF - IS-IS</li> <li>– NSF - OSPF</li> <li>– NSF - OSPF (RFC 3623 OSPF Graceful Restart)</li> <li>– NSF Awareness - EIGRP</li> <li>– NSF Awareness - OSPF</li> </ul> </li> <li>• NSF/SSO (Nonstop Forwarding with Stateful Switchover) <ul style="list-style-type: none"> <li>– NSF/SSO - GLBPv6</li> <li>– NSF/SSO - IPsec</li> <li>– NSF/SSO - IPv6 uRPF</li> <li>– NSF/SSO - Managed LNS MPLS</li> <li>– NSF/SSO - MLD Access Group</li> <li>– NSF/SSO - MPLS VPN</li> </ul> </li> </ul>

Table 1 Feature Information for Cisco Nonstop Forwarding (continued)

Feature Name	Releases	Feature Information
		The following commands were introduced or modified: <b>bgp graceful-restart</b> , <b>debug eigrp nsf</b> , <b>debug ip eigrp notifications</b> , <b>debug isis nsf</b> , <b>debug ospf nsf</b> , <b>ip cef distributed</b> , <b>nsf</b> (EIGRP), <b>nsf</b> (IS-IS), <b>nsf</b> (OSPF), <b>nsf interface wait</b> , <b>nsf interval</b> , <b>nsf t3</b> , <b>router bgp</b> , <b>router eigrp</b> , <b>router isis</b> , <b>router ospf</b> , <b>show cef nsf</b> , <b>show cef state</b> , <b>show clns neighbors</b> , <b>show ip bgp</b> , <b>show ip bgp neighbors</b> , <b>show ip cef</b> , <b>show ip ospf</b> , <b>show ip ospf neighbor</b> , <b>show ip protocols</b> , <b>show isis database</b> , <b>show isis nsf</b> , <b>timers nsf converge</b> , <b>timers nsf route-hold</b> , <b>timers nsf signal</b> .
NSF—OSPF (RFC 3623 OSPF Graceful Restart)	Cisco IOS XE Release 2.1	This document focuses on NSF for OSPFv2 in Cisco IOS XE software, using the IETF standardized graceful restart function as described in RFC 3623.  The following commands were introduced or modified: <b>nsf cisco</b> , <b>nsf ietf</b> , <b>nsf (OSPF)</b> .
NSF/SSO - HSRPv6	Cisco IOS XE Release 2.1	This feature was introduced.
NSF/SSO - HSRPv6 on VRF interfaces	Cisco IOS XE Release 3.1S	This feature was introduced for Cisco ASR 1000 Series Aggregation Services Routers.
NSF/SSO - Multicast MPLS VPN	Cisco IOS XE Release 2.5.	This feature was introduced.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1005R)

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

© 2002–2010 Cisco Systems, Inc. All rights reserved.





# Cisco IOS XE In Service Software Upgrade Process

---

**First Published: March 16, 2006**  
**Last Updated: July 23, 2010**

The Cisco IOS XE In Service Software Upgrade (ISSU) process allows Cisco IOS XE Software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS XE Software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for Performing the Cisco IOS XE ISSU Process](#)” section on [page 13](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE Software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Performing the Cisco IOS XE ISSU Process, page 2](#)
- [Restrictions for Performing the Cisco IOS XE ISSU Process, page 2](#)
- [Information About Performing the Cisco IOS XE ISSU Process, page 2](#)
- [How to Perform the Cisco IOS XE ISSU Process, page 9](#)
- [Configuration Examples for Performing the Cisco IOS XE ISSU Process, page 9](#)



- [Additional References, page 11](#)
- [Feature Information for Performing the Cisco IOS XE ISSU Process, page 13](#)

## Prerequisites for Performing the Cisco IOS XE ISSU Process

- Ensure that both the active and the standby Route Processors (RPs) are available in the system.
- The new and old Cisco IOS XE Software images must be loaded into the file systems of both the active and standby RPs before you begin the ISSU process.
- Stateful switchover (SSO) must be configured and working properly. For configuration information, see [Stateful Switchover](#).
- Nonstop forwarding (NSF) must be configured and working properly. For configuration information, see [Cisco Nonstop Forwarding](#).
- Cisco ASR 1002 and Cisco ASR1004 Routers must be booted in sub-package mode to perform an ISSU upgrade; Cisco ASR 1006 Routers can be booted in either consolidated package mode or sub-package mode.
- On the Cisco ASR 1006 Router, the standby router must be in the STANDBY HOT state before an ISSU upgrade starts.
- On the Cisco ASR 1002 and Cisco ASR 1004 Routers, Cisco IOS must reach the terminal SSO state before the ISSU upgrades starts.
- Before you perform ISSU, ensure the system is configured for redundancy-mode SSO and that the file system for both the active and standby RPs contains the new ISSU-compatible image. The current version running in the system must also support ISSU. You can issue various commands to determine RP versioning and compatibility, or you can use the ISSU application on Cisco Feature Navigator.

## Restrictions for Performing the Cisco IOS XE ISSU Process

### General Restrictions

- Do not make any hardware changes while performing an ISSU process.
- Even with ISSU, it is recommended that upgrades be performed during a maintenance window.
- The new features that require configuration changes should not be enabled during the ISSU process.
- In a downgrade scenario, if any feature is not available in the downgrade revision Cisco IOS XE Software image, that feature should be disabled prior to initiating the ISSU process.

### Cisco ASR 1000 Series Aggregation Services Routers Restrictions

For information about ISSU restrictions between hardware and software configurations on the Cisco ASR 1000 Series Router, see the [Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide](#).

## Information About Performing the Cisco IOS XE ISSU Process

- [ISSU Process Overview, page 3](#)

- [Overview of Stateful Switchover, page 4](#)
- [NSF Overview, page 6](#)
- [Versioning Capability in Cisco IOS XE Software to Support ISSU, page 7](#)
- [SNMP Support for ISSU, page 8](#)
- [ISSU-Capable Protocols and Applications, page 8](#)

## ISSU Process Overview

The ISSU process allows software to be updated or otherwise modified while packet forwarding continues with minimal interruption.

For the Cisco ASR 1000 Series Routers, ISSU-compatibility depends on the software sub-package being upgraded and the hardware configuration. Consolidated packages are ISSU-compatible in dual RP configurations only and have other limitations described in the [Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide](#).

Some RP and ESP software sub-packages can be upgraded using ISSU even in single RP or ESP hardware configurations via dual IOS processes running on the RP; others require dual RP or ESP configurations for an ISSU upgrade. The SPA and SIP software sub-packages must be upgraded on a per-SPA or per-SIP basis. See [Table 1](#) to view an ISSU table that addresses the contexts where limited interruption upgrades can be performed.

If you are updating multiple sub-packages, the sequence of the upgrade is important to minimize router downtime for the software upgrade.

The Cisco ASR 1000 Series Routers are designed to run one version of Cisco IOS XE Software for all consolidated packages and sub-packages on an RP, and running sub-packages from different versions of Cisco IOS XE Software can cause unexpected router behavior.

[Table 1](#) provides a list of the Cisco ASR 1000 Series Routers sub-packages and whether or not they can be upgraded without losing any network traffic in single and dual RP and ESP configurations using ISSU.

**Table 1** *Limited Interruption Upgrade Compatibility Table*

Sub-Package	Non-redundant RP and ESP	Redundant RP and ESP
Consolidated package (any)	No (Reload required)	Yes (RP switchover)
RPBase	No (RP Reload required)	Yes (RP switchover)
RPControl	Yes (in-service)	Yes (in-service)
RPAccess	Yes (in-service)	Yes (in-service)
RPIOS	Yes <sup>1</sup> (IOS software switchover)	Yes (RP switchover)
ESPBase	No <sup>2</sup> (ESP reload required)	Yes <sup>3</sup> (via ESP switchover)
SIPBase <sup>4</sup>	No (SPAs in SIP do not forward traffic during upgrade)	No (SPAs in SIP do not forward traffic during upgrade)
SIPSPA <sup>5</sup>	No (SPAs in SIP do not forward traffic during upgrade)	No (SPAs in SIP do not forward traffic during upgrade)

1. Only supported if software redundancy is configured on the RP.

2. ESP has to reload to complete ESPBase sub-package upgrade. All router traffic will be lost during ESP upgrade.

3. An ESP switchover occurs as part of the upgrade, so traffic is forwarded with minimal interruption.
4. Any SIPBase upgrade will require the SPA interfaces to go down during the upgrade for all the SPAs in the SIP.
5. Any SIPSPA upgrade will require the SPA interfaces for that particular SPA to go down during the upgrade.



---

**Note** ROMmon images are downloaded separately from Cisco IOS XE images and have their own installation procedures, and are not mentioned in this document as part of the ISSU upgrade procedure.

---

## ISSU Rollback Timer Overview on the Cisco ASR 1000 Series Router

The Cisco ASR 1000 Series Router ISSU procedure has a rollback timer. Rollback timers are used for for ISSU procedures on all Cisco routers that support ISSU.

During ISSU, the rollback timer begins after the consolidated package or sub-package is loaded. If the upgrade does not move forward in the amount of time specified in the rollback timer, the configuration will automatically “roll back” to the previous configuration and the ISSU upgrade will be cancelled.

For ISSU upgrades on Cisco ASR 1000 Series Routers, it may be advisable to set long rollback times when the upgrade is being performed on routers with large configurations.

## ISSU with Dual IOS Processes on a Single RP Overview

To complete an ISSU upgrade of an individual sub-package using dual IOS processes on a single RP, RPR or SSO must first be enabled.

ISSU with dual IOS processes is useful for upgrading the individual RP sub-packages that can be upgraded without a router reload. See [Table 1](#) for a list of these sub-packages. Most sub-package upgrades in a single RP configuration require a hardware reload to complete (whether an RP reload for an RP sub-package, an ESP reload for the ESPBase sub-package, a SIP reload for a SIPBase sub-package, or a SPA reload for the SIPSPA sub-package), so limited interruption upgrades for single RP configurations are not available in most upgrade scenarios.

## Overview of Stateful Switchover

Development of the SSO feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS XE routers.

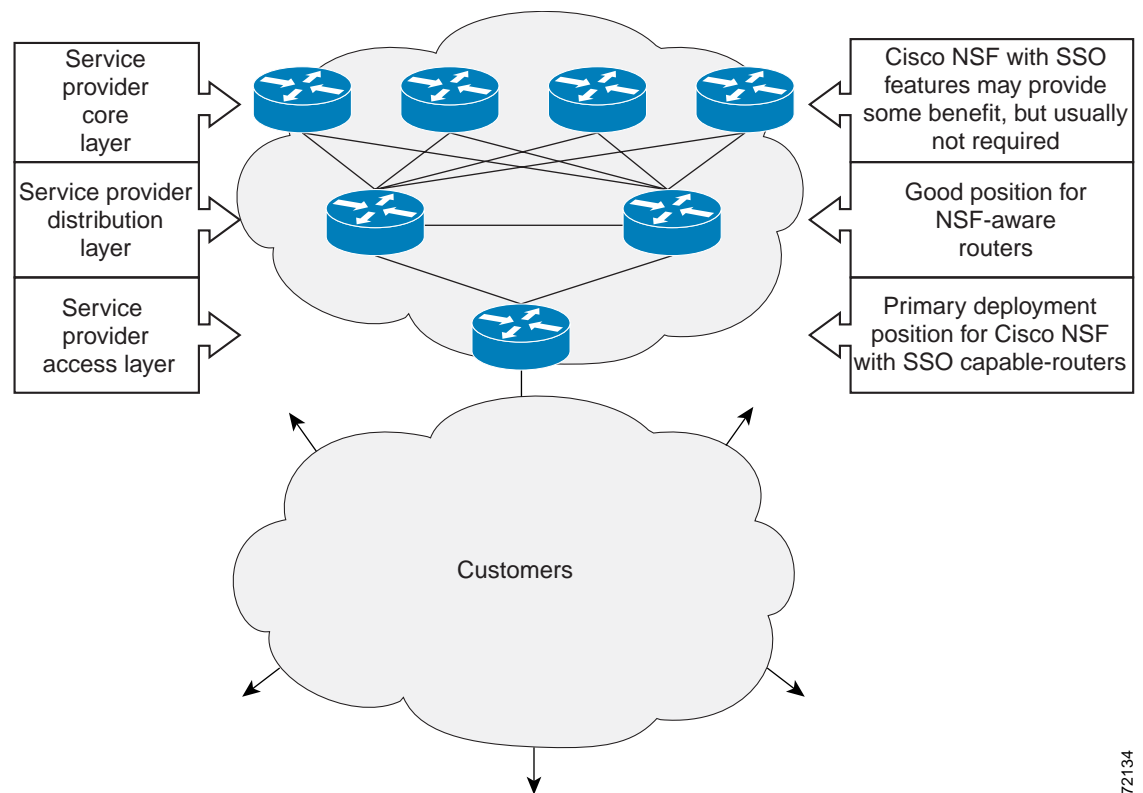
In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between 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. The Cisco 1000 ASR Series Routers also support dual IOS processes on a single RP to provide SSO capability.

Cisco NSF is used with SSO. 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.

Figure 1 illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is enabled 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.

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. Depending on your objectives, you may decide to deploy Cisco NSF and SSO features at the core layer of your network. Doing this can help reduce the time to restore network capacity and service for certain failures, which leads to additional availability.

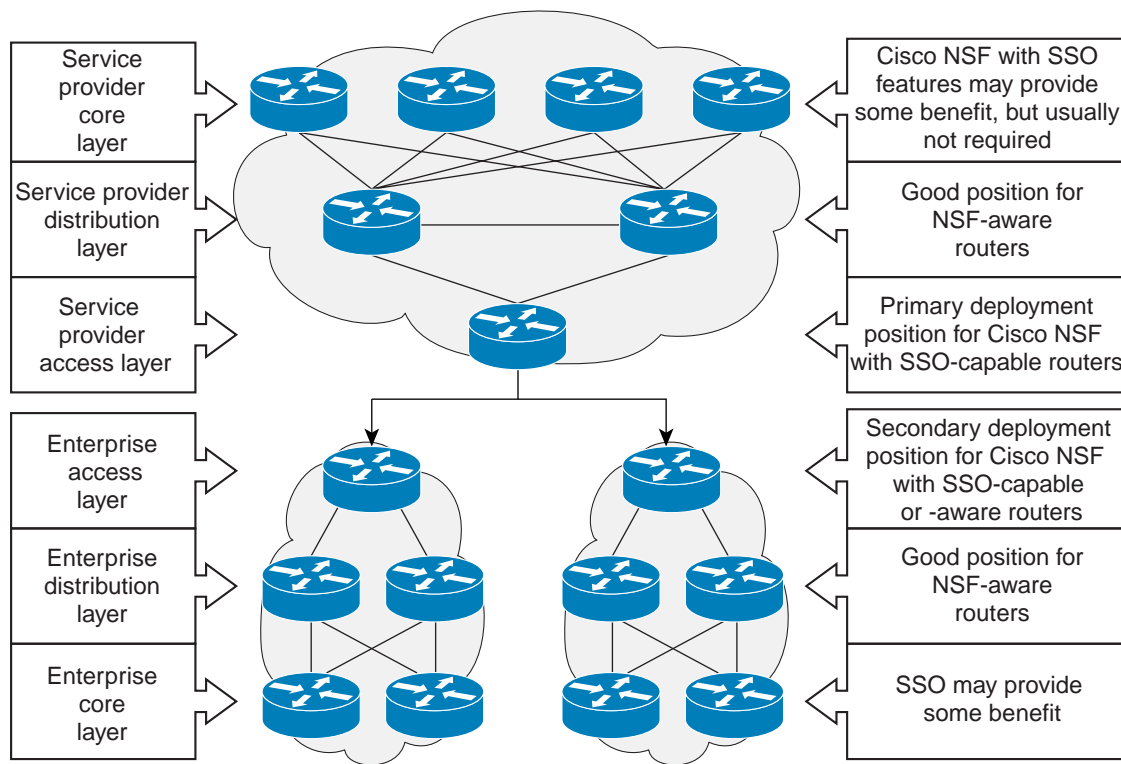
**Figure 1** Cisco NSF with SSO Network Deployment: Service Provider Networks



72134

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. Figure 2 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



72064

## NSF Overview

Cisco NSF works with the SSO feature in Cisco IOS XE Software. SSO is a prerequisite of Cisco NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco 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. Cisco NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

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 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 Cisco NSF operation.

## Versioning Capability in Cisco IOS XE Software to Support ISSU

Before the introduction of the ISSU capability, the SSO mode of operation required each RP to be running like-versions of Cisco IOS XE Software. The operating mode of the system in a redundant HA configuration is determined by exchanging version strings when the standby RP registers with the active RP.

The system entered SSO mode only if the versions running on both RPs were the same. If not, the redundancy mode was reduced to ensure compatibility. With ISSU capability, the implementation allows two different but compatible release levels of Cisco IOS XE images to interoperate in SSO mode and enables software upgrades while packet forwarding continues. Version checking done before ISSU capability was introduced is no longer sufficient to allow the system to determine the operating mode.

ISSU requires additional information to determine compatibility between software versions. Therefore, a compatibility matrix is defined that contains information about other images with respect to the one in question. This compatibility matrix represents the compatibility of two software versions, one running on the active and the other on the standby RP, and to allow the system to determine the highest operating mode it can achieve. Incompatible versions will not be able to progress to SSO operational mode.

The Cisco IOS XE infrastructure has been internally modified and redesigned to accommodate subsystem versioning with ISSU. Cisco IOS XE subsystems correspond to feature sets and software component groupings. Features or subsystems that maintain state information across RPs are HA-aware or SSO clients. A mechanism called ISSU Framework, or ISSU protocol, allows subsystems within Cisco IOS XE software to communicate RP to RP and to negotiate the message version for communication between RPs. Internally, all NSF- and SSO-compliant applications or subsystems that are HA-aware must follow this protocol to establish communication with their peer across different versions of software. For information about operating modes, see the “[Stateful Switchover](#)” module in the *Cisco IOS XE High Availability Configuration Guide*.

### Compatibility Matrix

You can perform the ISSU process when the Cisco IOS XE Software on both the active and the standby RP is capable of ISSU and the old and new images are compatible. The compatibility matrix information stores the compatibility among releases as follows:

- **Compatible**—The base-level system infrastructure and all optional HA-aware subsystems are compatible. An in-service upgrade or downgrade between these versions will succeed with minimal service impact. The matrix entry designates the images to be compatible (C).
- **Base-level compatible**—One or more of the optional HA-aware subsystems is not compatible. An in-service upgrade or downgrade between these versions will succeed; however, some subsystems will not be able to maintain state during the transition. The matrix entry designates the images to be base-level compatible (B).
- **Incompatible**—A core set of system infrastructure exists that must be able to interoperate in a stateful manner for SSO to function correctly. If any of these required features or protocols is not interoperable, then the two versions of the Cisco IOS XE Software images are declared to be incompatible. An in-service upgrade or downgrade between these versions is not possible. The matrix entry designates the images to be incompatible (I).

The compatibility matrix represents the compatibility relationship a Cisco IOS XE Software image has with all of the other Cisco IOS XE Software versions within the designated support window (for example, all of those software versions the image “knows” about) and is populated and released with every image. The matrix stores compatibility information between its own release and prior releases. It is always the newest release that contains the latest information about compatibility with existing

releases in the field. The compatibility matrix is available within the Cisco IOS XE Software image and on Cisco.com so that users can determine in advance whether an upgrade can be done using the ISSU process.

## SNMP Support for ISSU

ISSU - SNMP for SSO provides a mechanism for synchronizing the Simple Network Management Protocol (SNMP) configurations and the MIBs that support SSO from the active RP to the standby RP, assuming that both RPs are running the same version of Cisco IOS XE Software. This assumption is not valid for ISSU.

ISSU - SNMP provides an SNMP client that can handle ISSU transformations for the MIBs. An SNMP client (SIC) handles ISSU for all MIBs and handles the transmit and receive functions required for ISSU. During SNMP, a MIB is completely synchronized from the active RP to the standby RP only if the versions of the MIB on both Cisco IOS XE releases are the same.

## ISSU-Capable Protocols and Applications

The following protocols and applications support ISSU:

- FHRP - HSRP Group Shutdown—FHRP - HSRP group shutdown is supported in ISSU.
- ISSU - ARP—Address Resolution Protocol (ARP) is supported in ISSU.
- ISSU - ATM—Asynchronous Transfer Mode (ATM) is supported in ISSU. The application requirements for ISSU are as follows:
  - Identify the ATM client as nonbase
  - Support message versioning of ATM HA event synchronous messages
  - Provide capability exchange between peers
- Cisco Express Forwarding—Cisco Express Forwarding is supported in ISSU.
- ISSU - FHRP/GLBP—Cisco Gateway Load Balancing Protocol (GLBP) is supported in ISSU.
- ISSU - FHRP/HSRP—The Hot Standby Router Protocol (HSRP) is supported in ISSU.
- ISSU - GLBPv6—GLBP Version 6 is support in ISSU.
- ISSU - Frame Relay—The Frame Relay protocol is supported in ISSU.
- ISSU - HDLC—The High-Level Data Link Control (HDLC) protocol is supported in ISSU.
- ISSU - HSRPv6—HSRPv6 is supported in ISSU.
- ISSU - IGMP snooping—IGMP snooping is supported in ISSU.
- ISSU - IPv6 uRPF—IPv6 Unicast Reverse Path Forwarding (uRPF) is supported in ISSU.
- ISSU - IS-IS—The Intermediate System-to-Intermediate System (IS-IS) protocol is supported in ISSU.
- ISSU - Managed LNS MPLS—Managed L2TP network server (LNS) Multiprotocol Label Switching Protocol (MPLS), also know as VRF-Lite MPLS, is supported in ISSU.
- ISSU - MLD Access Group—Multicast Listener Discovery Protocol (MLD) access groups are supported in ISSU.
- ISSU - Multicast MPLS VPN—Multicast MPLS Virtual Private Networks (VPNs) are supported in ISSU.

- ISSU - NAT—Network Address Translation (NAT) is supported in ISSU.
- ISSU - PPP/MLP—Point-to-Point Protocol (PPP) and multilink PPP (MLP) support ISSU.
- ISSU - QoS support—The Quality of Service (QoS) feature is supported in ISSU.
- ISSU - Remote File System—The Remote File System (RFS) versioning feature is supported in ISSU.
- ISSU - SNMP—SNMP is supported in ISSU.
- ISSU - VRRP—VRRP is supported in ISSU.

**Note**

For a complete list of ISSU-capable protocols and application supported for the Cisco ASR 1000 Series Routers, see the [Release Notes for Cisco ASR 1000 Series Aggregation Services Routers](#).

## How to Perform the Cisco IOS XE ISSU Process

Unlike SSO, which is a mode of operation for the device and a prerequisite for performing ISSU, the ISSU process is a series of steps performed while the router or switch is in operation. The steps result in the implementation of new or modified Cisco IOS XE Software, and have a minimal impact to traffic.

For information on performing Cisco IOS XE ISSU upgrades on the Cisco ASR 1000 Series Router, see the “In Service Software Upgrade (ISSU)” chapter in the [Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide](#).

## Configuration Examples for Performing the Cisco IOS XE ISSU Process

- [Example: Verifying Redundancy Mode Before Beginning the ISSU Process, page 9](#)
- [Example: Verifying the ISSU State, page 10](#)

### Example: Verifying Redundancy Mode Before Beginning the ISSU Process

The following examples display verification that the system is in SSO mode and that slot R0 is the active RP1 and slot R1 is the standby RP1. Both RPs are running the same Cisco IOS XE Software image.

```
Router# show redundancy states

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

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

client count = 67
client_notification_TMR = 30000 milliseconds
```

```

RF debug mask = 0x0

Router# show platform

Chassis type: ASR1006

Slot      Type                State                Insert time (ago)
-----
0         ASR1000-SIP10         ok                   02:48:56
0/0       SPA-2X1GE-V2          ok                   02:46:38
0/1       SPA-2XOC3-POS         ok                   02:46:38
R0        ASR1000-RP1           ok, active           02:48:56
R1        ASR1000-RP1           ok, standby          02:48:56
F0        ASR1000-ESP10         ok, active           02:48:56
F1        ASR1000-ESP10         ok, standby          02:48:56
P0        ASR1006-PWR-AC        ok                   02:47:55
P1        ASR1006-PWR-AC        ok                   02:47:55

Slot      CPLD Version          Firmware Version
-----
0         07091401             12.2(33r)XN2
R0        07062111             12.2(33r)XN2
R1        07062111             12.2(33r)XN2
F0        07051680             12.2(33r)XN2
F1        07051680             12.2(33r)XN2

```

## Example: Verifying the ISSU State

The following example displays and verifies the ISSU state:

```

Router# show issu state detail

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

No ISSU operation is in progress

```

The new version of the Cisco IOS XE Software must be present on both of the RPs. The directory information displayed for each of the RPs shows that the new version is present.

```

Router# dir harddisk:

Directory of harddisk:/

 11 drwx      16384 Jul 24 2008 15:04:47 +00:00 lost+found
1114113 drwx      65536 Nov 25 2008 16:58:36 +00:00 tracelogs
294913 drwx      4096 Jul 24 2008 15:14:39 +00:00 core
 12 -rw-    225308932 Nov 12 2008 15:50:37 +00:00
asr1000rp1-adventerprisek9.02.02.00.122-33.XNB-20080810_010002-mcp_dev_2.bin
 13 -rw-    209227980 Aug 20 2008 17:31:59 +00:00 asr1000special
 14 -rw-    222240972 Sep 8 2008 17:13:22 +00:00 rp_super.ppc.bin
 15 -rw-    209985740 Nov 25 2008 16:50:39 +00:00
asr1000rp1-adventerprisek9.02.01.02.122-33.XNA2.bin

39313059840 bytes total (38439649280 bytes free)

Router# dir stby-harddisk:

Directory of stby-harddisk:/

 11 drwx      16384 Jul 24 2008 15:05:35 +00:00 lost+found

```

```

1507329 drwx      73728 Nov 25 2008 16:58:50 +00:00  tracelogs
2424833 drwx      4096  Jul 24 2008 15:22:04 +00:00  core
  12 -rw-    225308932 Sep 8 2008 04:48:39 +00:00
asr1000rp1-adventerprisek9.02.02.00.122-33.XNB-20080810_010002-mcp_dev_2.bin
  13 -rw-    209227980 Aug 20 2008 17:41:21 +00:00  asr1000special
  14 -rw-    222240972 Sep 8 2008 18:04:26 +00:00  rp_super.ppc.bin
  15 -rw-    209985740 Nov 25 2008 16:55:11 +00:00
asr1000rp1-adventerprisek9.02.01.02.122-33.XNA2.bin

39313059840 bytes total (38438928384 bytes free)

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS High Availability commands	<a href="#">Cisco IOS High Availability Command Reference</a>
Cisco nonstop forwarding	<a href="#">Cisco Nonstop Forwarding</a>
Stateful switchover	<a href="#">Stateful Switchover</a>
FHRP and HSRP group shutdown	“ <a href="#">Configuring HSRP</a> ” chapter of the <i>Cisco IOS XE IP Application Services Configuration Guide</i>
ISSU on the Cisco ASR 1000 Series Routers	“ <a href="#">In Service Software Upgrades</a> ” chapter of the <i>Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</i>
VRRP	“ <a href="#">Configuring VRRP</a> ” chapter in the <i>Cisco IOS XE IP Application Services Configuration Guide</i>

### Standards

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

### MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

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

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Performing the Cisco IOS XE ISSU Process

Table 2 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 2** Feature Information for the Cisco IOS XE ISSU Process

Feature Name	Releases	Feature Information
Cisco IOS XE In Service Software Upgrade (ISSU)	Cisco IOS XE Release 2.1	<p>The following features were introduced:</p> <ul style="list-style-type: none"> <li>• Dual IOS processes on the same RP</li> <li>• In Service Software Upgrade (ISSU) <ul style="list-style-type: none"> <li>– ISSU - ARP</li> <li>– ISSU - Frame Relay</li> <li>– ISSU - GLBPv6</li> <li>– ISSU - HSRPv6</li> <li>– ISSU - HDLC</li> <li>– ISSU - IGMP snooping</li> <li>– ISSU - IPv6 uRPF</li> <li>– ISSU - IS-IS</li> <li>– ISSU - Managed LNS MPLS</li> <li>– ISSU - MLD Access Group</li> <li>– ISSU - NAT</li> <li>– ISSU - PPP/MLP</li> <li>– ISSU - QoS</li> <li>– ISSU - SNMP</li> </ul> </li> </ul> <p>The following commands were introduced or modified  <b>issu abortversion, issu acceptversion, issu commitversion, issu loadversion, issu runversion, issu set rollback timer, show issu clients, show issu comp-matrix, show issu rollback timer, show issu sessions, show issu state, show redundancy.</b></p>
ISSU - ATM	Cisco IOS XE Release 2.3	This feature was introduced.

**Table 2**      *Feature Information for the Cisco IOS XE ISSU Process (continued)*

Feature Name	Releases	Feature Information
ISSU - HSRPv6 on VRF interfaces	Cisco IOS XE Release 3.1S	This feature was introduced for Cisco ASR 1000 Series Aggregation Services Routers.
ISSU - Multicast MPLS VPN	Cisco IOS XE Release 2.5	This feature was introduced.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1005R)

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

© 2006–2010 Cisco Systems, Inc. All rights reserved.



# AAA High Availability Support for Local PPPoX Sessions

---

**First Published:** November 20, 2006  
**Last Updated:** November 19, 2010

This feature enhances the authentication, authorization, and accounting (AAA) capability to meet high availability (HA) criteria for locally terminated Point-to-Point Protocol (PPP) over Ethernet (PPPoE) and PPPoEoX sessions, where X represents VLAN or QinQ. The following Feature Manager features are supported in this implementation of AAA HA:

- Absolute (session) timeout
- Idle timeout
- Access control lists (ACLs)
- ACL Filter
- Quality of service (QoS)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for AAA High Availability Support for Local PPPoX Sessions” section on page 7](#).

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Restrictions for AAA High Availability Support for Local PPPoX Sessions, page 2](#)



- [Information About AAA High Availability Support for Local PPPoX Sessions, page 2](#)
- [How to Configure AAA High Availability Support for Local PPPoX Sessions, page 4](#)
- [Additional References, page 5](#)
- [Additional References, page 5](#)
- [Feature Information for AAA High Availability Support for Local PPPoX Sessions, page 7](#)

## Restrictions for AAA High Availability Support for Local PPPoX Sessions

- If an administrator changes the protocol of a server group (for example, from RADIUS to TACACS+), HA will not be available for sessions configured to use that server group.
- IP sessions are not supported in this implementation of AAA HA.
- This implementation of AAA HA supports only locally terminated PPPoX sessions, including the following:
  - PPP over Ethernet (PPPoE)
  - PPPoE terminated into a multiprotocol label switching (MPLS) virtual private network (VPN)
  - PPPoEoE 802.1q into MPLS VPN
  - PPPoEoE 802.1q-in-q into MPLS VPN
  - Dynamic Host Configuration Protocol (DHCP) VPN ID option 82
  - Per VPN AAA
- The following Feature Manager features are not supported in this implementation of AAA HA:
  - Prepaid Time Monitor
  - Prepaid Volume Monitor
  - L4 Redirect
  - Traffic Classification
  - Portbundle Hostkey
  - IPv6 DHCP from AAA

## Information About AAA High Availability Support for Local PPPoX Sessions

- [AAA HA Enhancement, page 3](#)
- [HA and Authentication, page 3](#)
- [HA and Authorization, page 3](#)
- [HA and Accounting, page 3](#)

## AAA HA Enhancement

Cisco HA delivers carrier grade reliability with Cisco devices running Cisco IOS XE software. Carrier grade means that service disruption because of outages, service upgrades, or other maintenance activities on Cisco IOS XE platforms are rarely experienced. To achieve this level of service, Cisco uses two route processors to manage and control the sessions and services for each device. One processor is active and the other is in standby mode, ready to provide backup. A transition from the active processor to the standby processor is transparent to the end user, but not necessarily to the service provider.

The router must maintain the following information during transient component failures:

- Authentication status of clients
- Authorization status
- Accounting and billing information

To maintain this information during transitions to the standby processor, Cisco IOS XE software uses an HA replay model to re-create as much state and database information as possible between the active and standby devices. The HA replay model works within existing external AAA server protocols to achieve the desired behavior.

## HA and Authentication

For authentication, only the following state information is maintained: knowledge that a session authenticated on the active processor need not be reauthenticated on the standby processor. Each authentication protocol, such as local, TACACS+, or RADIUS, responds in its protocol-specific way to an authentication request from a standby device. All AAA client authentication replies on a standby device should be successful.

## HA and Authorization

The HA process for authorization data is different from the authentication process. The AAA server caches the authorization responses for the sessions in order to provide the appropriate authorization attributes to AAA clients during a session replay. AAA clients use the authorization attributes to create a session copy on the standby route processor.

## HA and Accounting

The AAA HA accounting framework takes advantage of existing AAA features such as system accounting and periodic accounting to limit the loss of accounting and billing information caused by a switchover between an active processor and a standby processor.

## System Accounting

System accounting is a separate accounting capability that informs AAA servers about the state of a client device, such as a router. The AAA server receives a “System-Off” message when a controlled restart takes place on a client device. The message notifies the AAA server to clear any active sessions being managed for the specified client. When the client restarts and becomes available for new sessions, the AAA server receives a “System-On” message. The “System-On” message is also sent following uncontrolled restarts caused by device failures or other events that do not generate a “System-Off”

message. In either case, the AAA server no longer maintains any active sessions for the specified client device. The server bills or accounts for the sessions prior to the “System-On” message and starts a new session.

AAA’s accounting HA solution does not add any new requirements to system accounting for AAA servers. Any switchover will look like a very fast, minimally disruptive outage. Although end users do not experience any loss of service during an HA switchover, AAA servers reset their sessions and restart accounting for all switched-over sessions.

## Periodic Accounting

You can use periodic accounting to dynamically update records of session utilization for billing purposes. Periodic accounting minimizes the loss of usage statistics. HA does not eliminate the need to configure periodic accounting on a device if you require dynamic usage statistics for billing purposes. To achieve the HA level of reliability, the existing network topology configuration must be maintained.

# How to Configure AAA High Availability Support for Local PPPoX Sessions

- [Configuring AAA High Availability Support for Local PPPoX Sessions, page 4](#)
- [Troubleshooting an AAA High Availability Configuration, page 4](#)

## Configuring AAA High Availability Support for Local PPPoX Sessions

There are no configuration tasks associated with this feature. If you maintain your network topology for HA, then the AAA functions automatically participate in the HA feature for locally terminated PPPoX sessions.

## Troubleshooting an AAA High Availability Configuration

### SUMMARY STEPS

1. **enable**
2. **debug aaa redundancy**
3. **disable**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  Example: Router> enable	Enters the privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password, if prompted to do so.</li> </ul>
Step 2	<b>debug aaa redundancy</b>  Example: Router# debug aaa redundancy	Displays AAA synchronization data for the session synchronization to the standby device.
Step 3	<b>disable</b>  Example: Router# disable	Exits to user EXEC mode.

## Additional References

### Related Documents

Related Topic	Document Title
AAA commands	<a href="#">Cisco IOS Security Command Reference</a>
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS debug commands	<a href="#">Cisco IOS Debug Command Reference</a>
Authentication, Authorization, and Accounting (AAA)	“Authentication, Authorization, and Accounting (AAA)” section of the <a href="#">Security Configuration Guide: Securing User Services</a>

### Standards

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

### MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

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

## Technical Assistance

Description	Link
The Cisco 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for AAA High Availability Support for Local PPPoX Sessions

[Table 1](#) lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 1](#) lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 1** Feature Information for AAA HA Support for Local PPPoX Sessions

Feature Name	Releases	Feature Information
AAA High Availability Support for Local PPPoX Sessions	Cisco IOS XE Release 2.1	This feature enhances the AAA capability to meet HA criteria for locally terminated PPPoE and PPPoEoX sessions.  The following command was introduced or modified: <b>debug aaa redundancy.</b>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1005R)

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

© 2006—2010 Cisco Systems, Inc. All rights reserved.

