High Availability Configuration Guide, Cisco IOS XE 17.x

First Published: 2022-11-05

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

© 2022 Cisco Systems, Inc. All rights reserved.

CONTENTS

Full Cisco Trademarks with Software License

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

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

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

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

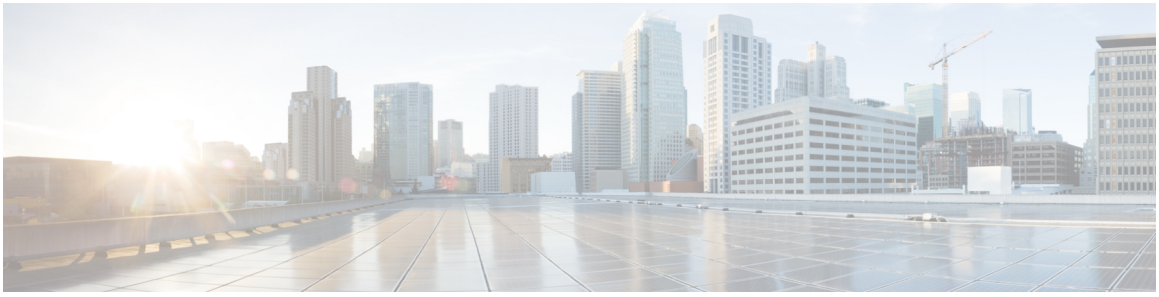
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

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

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

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



Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Audience and Scope

This document is designed for the person who is responsible for configuring your Cisco Enterprise router. This document is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- System administrators familiar with the fundamentals of router-based internetworking but who might not be familiar with Cisco IOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

Feature Compatibility

For more information about the Cisco IOS XE software, including features available on your device as described in the configuration guides, see the respective router documentation set.

To verify support for specific features, use the Cisco Feature Navigator tool. This tool enables you to determine the Cisco IOS XE software images that support a specific software release, feature set, or a platform.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

The command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example, see the following table.

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. Exclamation points are also displayed by the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

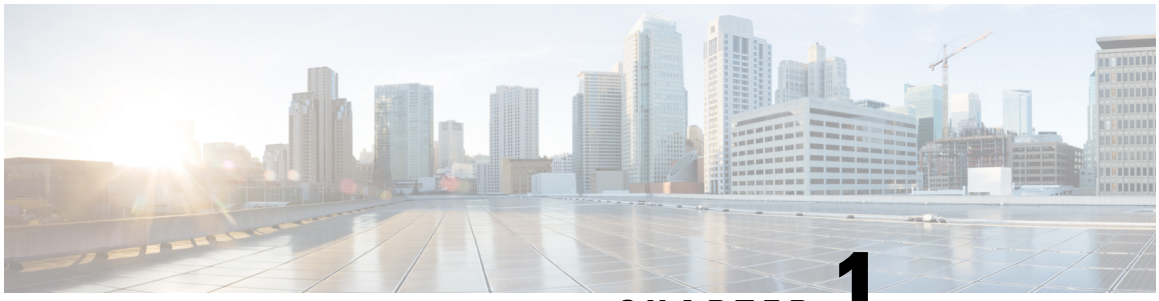
Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.



CHAPTER 1

Configuring Stateful Switchover

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

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

Prerequisites for Stateful Switchover

General Prerequisites

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

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

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

Restrictions for Stateful Switchover

General Restrictions for SSO

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

Configuration Mode Restrictions

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

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

Switchover Process Restrictions

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

Frame Relay and Multilink Frame Relay Restrictions

- The following Frame Relay features are not synchronized between the active and standby RPs in this release: Frame Relay statistics; enhanced LMI (ELMI); Link Access Procedure, Frame Relay (LAPF); SVCs; and subinterface line state.

Note The subinterface line state is determined by the PVC state, which follows the line card protocol state on DCE interfaces, and is learned from first LMI status exchange after switchover on DTE interfaces.

- Frame Relay SSO is supported with the following features:
  - Serial interfaces
  - DTE and DCE LMI (or no keepalives)
  - PVCs (terminated and switched)
  - IP
- When no LMI type is explicitly configured on a DTE interface, the autosensed LMI type is synchronized.

- LMI sequence numbers are not synchronized between the active and standby RPs by default.

LMI keepalive messages contain sequence numbers so that each side (network and peer) of a PVC can detect errors. An incorrect sequence number counts as one error. By default, the switch declares the line protocol and all PVCs down after three consecutive errors. Although it seems that synchronizing LMI sequence numbers might prevent dropped PVCs, the use of resources required to synchronize LMI sequence numbers for potentially thousands of interfaces (channelized) on larger networking devices might be a problem in itself. The networking device can be configured to synchronize LMI sequence numbers. Synchronization of sequence numbers is not necessary for DCE interfaces.

- Changes to the line protocol state are synchronized between the active and standby RPs. The line protocol is assumed to be up on switchover, providing that the interface is up.
- PVC state changes are not synchronized between the active and standby RPs. The PVC is set to the up state on switchover provided that the line protocol state is up. The true state is determined when the first full status message is received from the switch on DTE interfaces.
- Subinterface line state is not synchronized between the active and standby RPs. Subinterface line state is controlled by the PVC state, by configuration settings, or by the hardware interface state when the PVC is up. On switchover, the subinterface state is set to up, providing that the subinterfaces are not shut down and the main interface is up and the line protocol state is up. On DTE devices, the correct state is learned after the first LMI status exchange.
- Dynamic maps are not synchronized between the active and standby RPs. Adjacency changes as a result of dynamic map change are relearned after switchover.
- Dynamically learned PVCs are synchronized between the active and standby RPs and are relearned after the first LMI status exchange.
- For Multilink Frame Relay bundle links, the state of the local bundle link and peer bundle ID is synchronized.
- For a Multilink Frame Relay bundle, the peer ID is synchronized.

PPP Restrictions

- The following PPP features are not supported: dialer; authentication, authorization, and accounting (AAA), IPPOOL, Layer 2 (L2X), Point-to-Point Tunneling Protocol (PPTP), Microsoft Point-to-point Encryption (MPPE), Link Quality Monitoring (LQM), link or header compression, bridging, asynchronous PPP, and XXCP.

Cisco ASR 1000 Series Aggregation Services Routers Restrictions

- Only RPR and SSO are supported on Cisco ASR 1000 Aggregation Services routers.
- RPR and SSO can be used on Cisco ASR 1000 Aggregation Services routers to enable a second Cisco software process on a single RP. This configuration option is only available on Cisco ASR1001, ASR1001-X, ASR1002-X, ASR1001-HX, ASR1002-HX, ASR 1002 and ASR 1004 routers. On all other Cisco ASR 1000 Aggregation Services routers, the second Cisco software process can run on the standby RP only.
- A second Cisco software process can only be enabled using RPR or SSO if the RP is using 8 GB of DRAM. The **show version** command output shows the amount of DRAM configured on the router.

- Enabling software redundancy on the Cisco ASR1001-X, ASR1002-X, ASR1001-HX, ASR1002-HX,ASR 1001, ASR 1002, and ASR 1004 routers can reduce the Cisco IOS memory by more than half and adversely affect control plane scalability. We recommend that you use hardware redundant platforms, such as the Cisco ASR1006-X, ASR1009-X, ASR 1006 or ASR 1013 routers, in networks where both scalability and high availability are critical.
- Cisco ASR 1000 Series Router software redundancy requires an RTU license (FLASR1-IOSRED-RTU(=) on ASR 1002; and FLSASR1-IOSRED(=) on ASR 1001, ASR 1001-X, ASR 1001-HX, ASR 1002-HX, and ASR 1002-X), which allows you to enable software redundancy on the Cisco ASR 1001, ASR 1002, ASR 1001-X, ASR 1001-HX, ASR 1002-HX, ASR 1002-X, and ASR 1004 chassis. Software redundancy requires 4-GB DRAM on the RP1, and minimum 8-GB DRAM on the ASR 1001, ASR 1001-X, ASR 1001-HX, or ASR 1002-X. The Cisco ASR 1001, ASR 1002, and ASR 1002-X come by default with 4-GB DRAM on the built-in route processor, the ASR 1001-X and ASR 1001-HX come by default with 8-GB DRAM, and the ASR 1002-HX comes by default with 16-GB DRAM.

Information About Stateful Switchover

SSO Overview

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

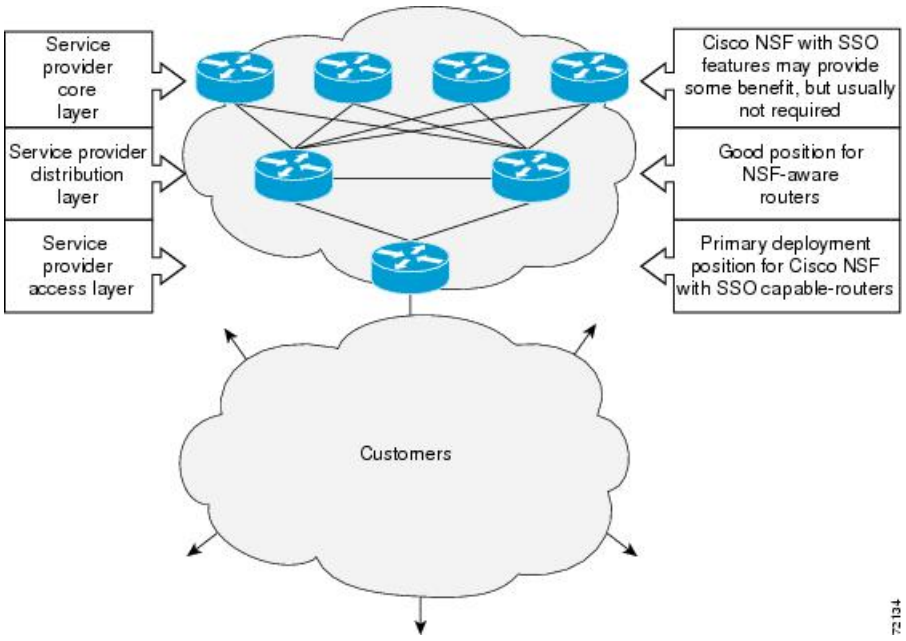
In Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between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

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

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

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

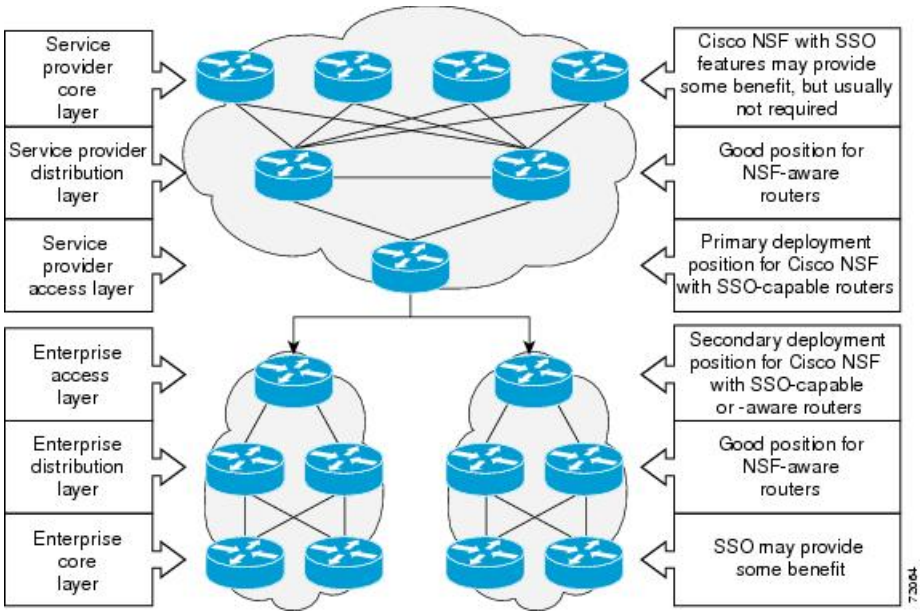
Figure 1: Cisco NSF with SSO Network Deployment: Service Provider Networks



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

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

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



Redundancy Modes

Route Processor Redundancy Mode

Router Processor Redundancy (RPR) allows Cisco software to be booted on the standby processor prior to switchover (a cold boot). In RPR, the standby RP loads a Cisco software 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.

Route Processor Synchronization

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

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

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

Bulk Synchronization During Initialization

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

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

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

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

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

Incremental Synchronization

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

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

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

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

Routing and forwarding information is synchronized to the standby RP:

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

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

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

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

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

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

Switchover Operation

Switchover Conditions

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

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

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

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

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

Switchover Time

The time required by the device to switch over from the active RP to the standby RP varies by platform:

Although the newly active processor takes over almost immediately following a switchover, the time required for the device to begin operating again in full redundancy (SSO) mode can be several minutes, depending on the platform. The length of time can be due to a number of factors including the time needed for the previously active processor to obtain crash information, load code and microcode, and synchronize configurations between processors and line protocols and Cisco NSF-supported protocols.

Core Dump Operation

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

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

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

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

Virtual Template Manager for SSO

The virtual template manager feature for SSO provides virtual access interfaces for sessions that are not HA-capable and are not synchronized to the standby router. The virtual template manager uses a redundancy facility (RF) client to allow the synchronization of the virtual interfaces in real time as they are created.

The virtual databases have instances of distributed FIB entries on line cards. Line cards require synchronization of content and timing in all interfaces to the standby processor to avoid incorrect forwarding. If the virtual access interface is not created on the standby processor, the interface indexes will be corrupted on the standby router and line cards, which will cause problems with forwarding.

SSO-Aware Protocols and Applications

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

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

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

Line Protocols

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

Frame Relay and Multilink Frame Relay Stateful Switchover

With stateful switchover, Frame Relay and Multilink 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 and Multilink 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 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 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 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 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 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.

APS

SSO support allow the automatic protection switching (APS) state to be preserved in the event of failover.

Routing Protocols and Nonstop Forwarding

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

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

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

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

Network Management

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

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

SSO for Circuit Emulation Services

SSO for circuit emulation services (CES) for TDM pseudowires provides the ability to switch an incoming DS1/T1/E1 on one SPA to another SPA on same SIP or onto a different SIP.

How to Configure Stateful Switchover

Copying an Image onto an RP

SUMMARY STEPS

1. **enable**
2. **copy tftp** {**slot** | **disk**}*device-number* **:** *filename*
3. **copy tftp** {**slave** | **stby-**}{**slot** | **disk**}*device-number* **:** *filename*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy tftp** {**slot** | **disk**}*device-number* **:** *filename* **Example:**	Copies a Cisco software image onto the flash device of the active RP.

	Command or Action	Purpose
	`Router# copy tftp slot0:image1`	
Step 3	**copy tftp** {**slave** | **stby-**}{**slot** | **disk**}*device-number* **:** *filename* **Example:** `Router# copy tftp stby-slot0:image1`	Copies a Cisco software image onto the flash device of the standby RP.
Step 4	**exit** **Example:** `Router# exit`	Exits to user EXEC mode.

Configuring SSO

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.

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

Configuring Frame Relay and Multilink Frame Relay Autosynchronization LMI Sequence Numbers

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**frame-relay redundancy auto-sync lmi-sequence-numbers** **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

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

Troubleshooting Stateful Switchover

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

This is normal behavior. Until the FSU procedure is complete, each RP will be running a different software version.

- You can enter ROM monitor mode by restarting the router and then pressing the Break key or issuing a **send break** command from a telnet session during the first 60 seconds of startup.The send break function can be useful for experienced users or for users under the direction of a Cisco Technical Assistance Center (TAC) representative to recover from certain system problems or to evaluate the cause of system problems.

Troubleshooting SSO

SUMMARY STEPS

1. **enable**
2. **crashdump-timeout** [*mm* | *hh* **:** *mm*]
3. **debug atm ha-error**
4. **debug atm ha-events**
5. **debug atm ha-state**
6. **debug ppp redundancy** [**detailed** | **event**]
7. **debug redundancy** {**all** | **ui** | **clk** | **hub**}
8. **show diag** [*slot-number* | **chassis** | **subslot** *slot* / *subslot*] [**details** | **summary**]
9. **show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **switchover history** | **states** | **inter-device**]
10. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**crashdump-timeout** [*mm* | *hh* **:** *mm*] **Example:** `router(config-red)# crashdump-timeout`	Set the longest time that the newly active RP will wait before reloading the formerly active RP.
Step 3	**debug atm ha-error** **Example:** `Router# debug atm ha-error`	Debugs ATM HA errors on the networking device.
Step 4	**debug atm ha-events** **Example:** `Router# debug atm ha-events`	Debugs ATM HA events on the networking device.

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco High Availability commands	*Cisco IOS High Availability Command Reference*
DHCP proxy client	ISSU and SSO--DHCP High Availability Features module in the *Cisco IOS IP Addressing Services Configuration Guide*

Related Topic	Document Title
MPLS high availability	MPLS High Availability: Overview module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO - 802.3ah OAM Support	Using Ethernet Operations, Administration, and Maintenance module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO - Any Transport over MPLS (AToM)	Any Transport over MPLS and AToM Graceful Restart module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO - E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the *Cisco IOS Carrier Ethernet Configuration Guide*
SSO - BFD (Admin Down)	Bidirectional Forwarding Detection module in the *Cisco IOS IP Routing: BFD Configuration Guide*
SSO GLBP	GLBP SSO module in the *Cisco IOS IP Application Services Configuration Guide*
SSO HSRP	Configuring HSRP module in the *Cisco IOS IP Application Services Configuration Guide*
SSO VRRP	Configuring VRRP module in the *Cisco IOS IP Application Services Configuration Guide*
Basic IPv6 configuration	Implementing IPv6 Addressing and Basic Connectivity module in the *Cisco IOS IPv6 Configuration Guide*
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

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

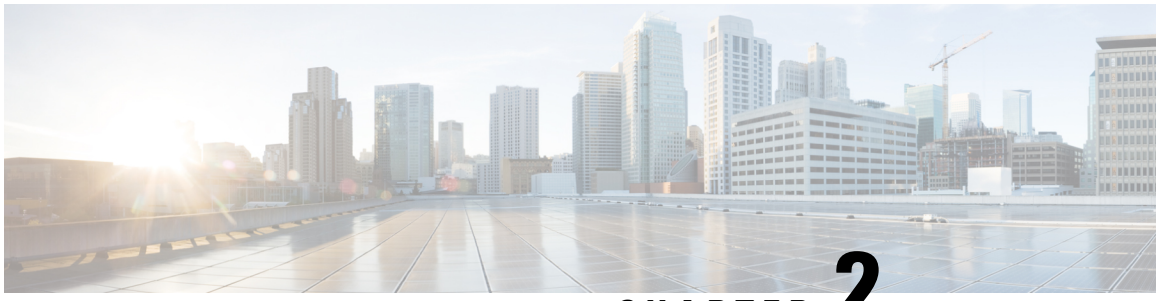
MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported 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.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 2

Configuring Nonstop Forwarding

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

The following terms are used throughout this document:

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

Prerequisites for Nonstop Forwarding

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

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

Restrictions for Nonstop Forwarding

General Restrictions

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

BGP NSF Restrictions

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

EIGRP NSF Restrictions

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

OSPF NSF Restrictions

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

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

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

Information About Nonstop Forwarding

Nonstop Forwarding

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

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

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

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

The NSF feature provides the following benefits:

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

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

Cisco NSF Routing and Forwarding

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

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

Cisco Express Forwarding and NSF

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

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

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

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

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

BGP NSF Operations

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

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

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

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

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

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

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

EIGRP NSF Operations

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

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

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

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

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

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

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

IPv6 support for NSF Operations

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

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

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

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

Nonstop Forwarding for IPv6 RIP

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

Nonstop Forwarding for Static Routes

Cisco NSF supports IPv6 static routes.

IS-IS NSF Operations

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

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

- IETF IS-IS
- Cisco IS-IS

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

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

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

IETF IS-IS Configuration

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

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

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

Cisco IS-IS Configuration

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

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

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

NSF-OSPF Operations

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

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

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

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

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

How to Configure Nonstop Forwarding

Configuring and Verifying BGP NSF

Repeat this procedure on each peer device.

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 or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 120`	Enables a BGP routing process, and enters router configuration mode.
Step 4	**bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] **Example:** `Router(config-router)# bgp graceful-restart`	Enables the BGP graceful restart capability, which starts NSF for BGP.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 6	**show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy**[**detail**]]] **Example:** `Router# show ip bgp neighbors`	Displays information about BGP and TCP connections to neighbors.

Configuring and Verifying EIGRP NSF

Repeat this procedure on each peer device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **nsf**
5. **timers nsf converge** *seconds*

6. **timers nsf signal** *seconds*
7. **timers nsf route-hold** *seconds*
8. **timers graceful-restart purge-time** *seconds*
9. **end**
10. **show ip protocols**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 109`	Enables an EIGRP routing process, and enters router configuration mode.
Step 4	**nsf** **Example:** `Router(config)# no nsf`	(Optional) Enables NSF capabilities. • This command is enabled by default.
Step 5	**timers nsf converge** *seconds* **Example:** `Router(config-router)# timers nsf converge 120`	(Optional) Adjusts the maximum time that the restarting device will wait for the EOT notification from an NSF-capable or NSF-aware peer. • Enter this command on NSF-capable devices only.
Step 6	**timers nsf signal** *seconds* **Example:** `Router(config-router)# timers nsf signal 20`	(Optional) Adjusts the maximum time for the initial restart period. • Enter this command on NSF-capable devices only.
Step 7	**timers nsf route-hold** *seconds* **Example:** `Router(config-router)# timers nsf route-hold 240`	(Optional) Sets the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer.

	Command or Action	Purpose
Step 8	**timers graceful-restart purge-time** *seconds* **Example:** `Router(config-router)# timers graceful-restart purge-time 240`	(Optional) Sets the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer.
Step 9	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 10	**show ip protocols** **Example:** `Router# show ip protocols`	Displays the parameters and current state of the active routing protocol process.

Configuring NSF-OSPF

Perform only one of the following tasks:

Configuring Cisco NSF-OSPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf cisco** [**enforce global**]
5. **nsf cisco helper** [**disable**]
6. **nsf ietf helper** [**disable** | **strict-lsa-checking**]
7. **end**
8. **show ip ospf nsf**

DETAILED STEPS

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

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

Configuring IETF NSF-OSPF

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. **nsf cisco helper disable**
7. **end**
8. **show ip ospf nsf**

DETAILED STEPS

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

Configuring and Verifying IS-IS NSF

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 7	**nsf interface wait** *seconds* **Example:** `Router(config-router)# nsf interface wait 15`	(Optional) Specifies how long a Cisco NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart. • This command is supported for Cisco NSF only.
Step 8	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 9	**show isis nsf** **Example:** `Router# show isis nsf`	Displays current state information regarding IS-IS NSF.

Troubleshooting Nonstop Forwarding

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 or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**debug eigrp nsf** **Example:** `Device# debug eigrp nsf`	Displays notifications and information about NSF events for an EIGRP routing process.
Step 3	**debug ip eigrp notifications** **Example:** `Device# debug ip eigrp notifications`	Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.
Step 4	**debug isis nsf** [**detail**] **Example:** `Device# debug isis nsf [detail]`	Displays information about the IS-IS state during a Cisco NSF restart.
Step 5	**debug ospf nsf** [**detail**] **Example:** `Device# debug ospf nsf [detail]`	Displays debugging messages related to OSPF Cisco NSF commands.
Step 6	**show cef nsf** **Example:** `Device# show cef nsf`	Displays the current NSF state of CEF on both the active and standby RPs.
Step 7	**show cef state** **Example:** `Device# show cef state`	Displays the CEF state on a networking device.
Step 8	**show clns neighbors** **Example:** `Device# show clns neighbors`	Displays both end system and intermediate system neighbors.
Step 9	**show ip bgp** **Example:** `Device# show ip bgp`	Displays entries in the BGP routing table.
Step 10	**show ip bgp neighbor** **Example:** `Device# show ip bgp neighbor`	Displays information about the TCP and BGP connections to neighbor devices.

	Command or Action	Purpose
Step 11	**show ip cef** **Example:** `Device# show ip cef`	Displays entries in the FIB that are unresolved, or displays FIB summary.
Step 12	**show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**] **Example:** `Device# show ip eigrp neighbors detail`	Displays displayed information about neighbors discovered by EIGRP.
Step 13	**show ip ospf** **Example:** `Device# show ip ospf`	Displays general information about OSPF routing processes.
Step 14	**show ip ospf neighbor** [**detail**] **Example:** `Device# show ip ospf neighbor [detail]`	Displays OSPF-neighbor information on a per-interface basis.
Step 15	**show ip protocols** **Example:** `Device# show ip protocols`	Displays the parameters and current state of the active routing protocol process. • The status of EIGRP NSF configuration and support is displayed in the output.
Step 16	**show isis database** [**detail**] **Example:** `Device# show isis database [detail]`	Displays the IS-IS link-state database.
Step 17	**show isis nsf** **Example:** `Device# show isis nsf`	Displays the current state information regarding IS-IS NSF.

Configuration Examples for Nonstop Forwarding

Example NSF-Capable CEF

The CEF NSF feature operates by default while the 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 the default or user-defined value for the route-hold timer is displayed.
- “EIGRP NSF enabled” or “EIGRP NSF disabled” appears in the output only when the NSF capability is supported by the device.

```
Device# show ip protocols

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

Example: Configuring Cisco NSF-OSPF

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

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

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

```
Device> show ip ospf nsf

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

Example: Configuring IETF NSF-OSPF

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

```
Device> enable
Device# configure terminal
```

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

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

```
Device> show ip ospf nsf

Routing Process "ospf 500"
Non-Stop Forwarding enabled
IETF NSF helper support enabled
Cisco NSF helper support disabled
  OSPF restart state is NO_RESTART
  Handle 1786466333, Router ID 10.1.1.1, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Example IS-ISNSF

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

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

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

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

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

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

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

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

```
Router# show isis nsf
NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
```

```
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco debug commands	*Cisco IOS Debug Command Reference*
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*
BGP support for NSF	BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) module in the *Cisco IOS IP Routing: BGP Configuration Guide*
EIGRP NSF awareness	EIGRP Nonstop Awareness module in the *Cisco IOS IP Routing: EIGRP Configuration Guide*
IPv6 BGP graceful restart	Implementing Multiprotocol BGP for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*

Related Topic	Document Title
IPv6 RIP	Implementing RIP for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
IPv6 static routes	Implementing Static Routes for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
NSF/SSO--802.3ah OAM Support	Using Ethernet Operations, Administration, and Maintenance module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO--Any Transport over MPLS (AToM)	Any Transport over MPLS and AToM Graceful Restart module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO--E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO--MPLS VPN	Configuring NSF/SSO--MPLS VPN module in the *MPLS Configuration Guide*
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3623	*Graceful OSPF Restart*
RFC 3847	*Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
RFC 4781	*Graceful Restart Mechanism for BGP*

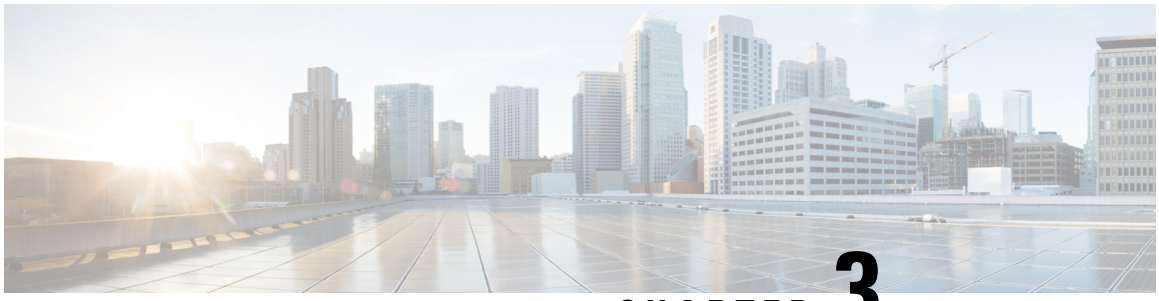
Technical Assistance

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

Feature Information for Nonstop Forwarding

The following table provides release information about the feature or features described in this module. This table 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.

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



CHAPTER 3

Performing an In Service Software Upgrade

This module describes the In Service Software Upgrade (ISSU) process and provides configuration examples for ISSU on Cisco ASR 1000 Series routers.

Information About Performing an ISSU

ISSU Process Overview

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

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

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

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

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

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

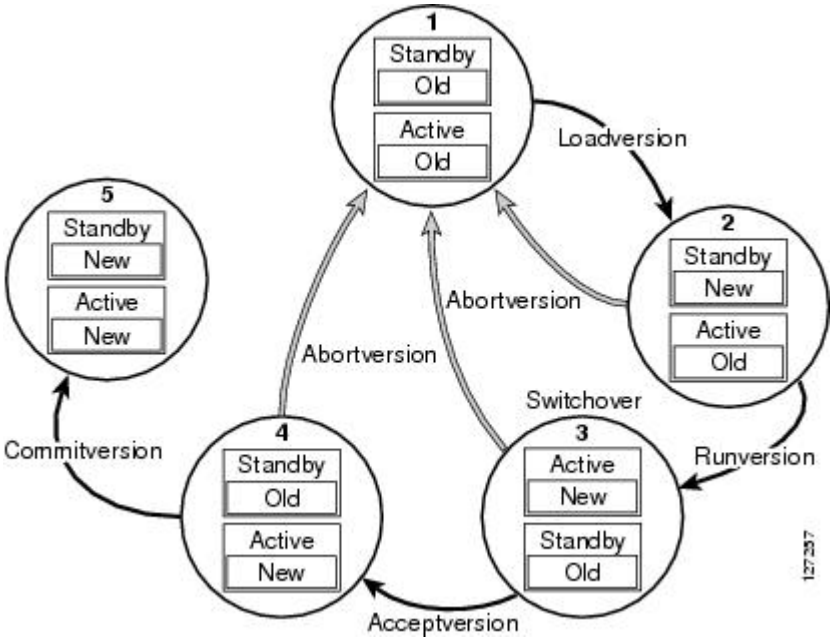
The two RPs in a system can be in one of three different states during ISSU:

- Active--One RP is actively forwarding packets with old software. After the ISSU process is performed, the original active RP becomes the standby RP.

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

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

Figure 3: ISSU States During the ISSU Process



How to Perform an ISSU

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 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 "Software Upgrade Process" section in the*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.

Configuration Examples for Performing an ISSU

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	Cisco IOS Master Commands List, All Releases
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*
FHRP and HSRP group shutdown	Configuring HSRP chapter of the *Cisco IOS XE IP Application Services Configuration Guide*
VRRP	Configuring VRRP chapter in the *Cisco IOS XE IP Application Services Configuration Guide*

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: http://www.cisco.com/go/mibs

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.	--

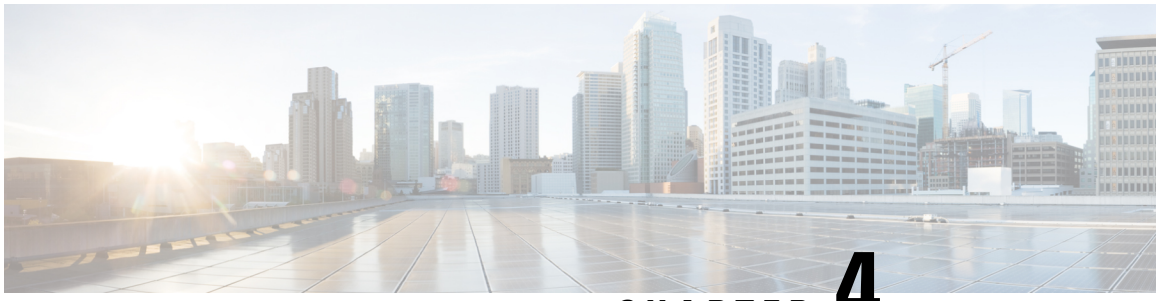
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Performing an XE ISSU

The following table provides release information about the feature or features described in this module. This table 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.

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



CHAPTER 4

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. 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)

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

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

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	**enable** **Example:** `Router> enable`	Enters the privileged EXEC mode. • Enter your password, if prompted to do so.
Step 2	**debug aaa redundancy** **Example:** `Router# debug aaa redundancy`	Displays AAA synchronization data for the session synchronization to the standby device.
Step 3	**disable** **Example:** `Router# disable`	Exits to user EXEC mode.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco debug commands	*Cisco IOS Debug Command Reference*
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*
BGP support for NSF	BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) module in the *Cisco IOS IP Routing: BGP Configuration Guide*
EIGRP NSF awareness	EIGRP Nonstop Awareness module in the *Cisco IOS IP Routing: EIGRP Configuration Guide*
IPv6 BGP graceful restart	Implementing Multiprotocol BGP for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*

Related Topic	Document Title
IPv6 RIP	Implementing RIP for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
IPv6 static routes	Implementing Static Routes for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
NSF/SSO--802.3ah OAM Support	Using Ethernet Operations, Administration, and Maintenance module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO--Any Transport over MPLS (AToM)	Any Transport over MPLS and AToM Graceful Restart module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO--E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO--MPLS VPN	Configuring NSF/SSO--MPLS VPN module in the *MPLS Configuration Guide*
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3623	*Graceful OSPF Restart*
RFC 3847	*Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
RFC 4781	*Graceful Restart Mechanism for BGP*

Technical Assistance

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

Feature Information for AAA High Availability Support for Local PPPoX Sessions

The following table provides release information about the feature or features described in this module. This table 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.

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