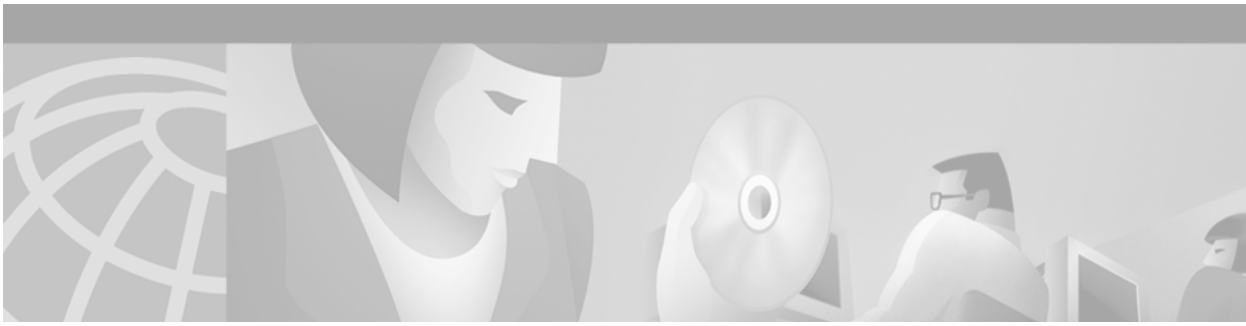


Stateful Switchover

Feature History

Release	Modification
12.0(22)S	This feature was introduced.

This document describes the Stateful Switchover (SSO) feature in Cisco IOS Release 12.0(22)S. It includes the following sections:

Note

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

is particularly useful at the network edgeSSO provides protection for network edge devices with dual Route Processors (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 specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

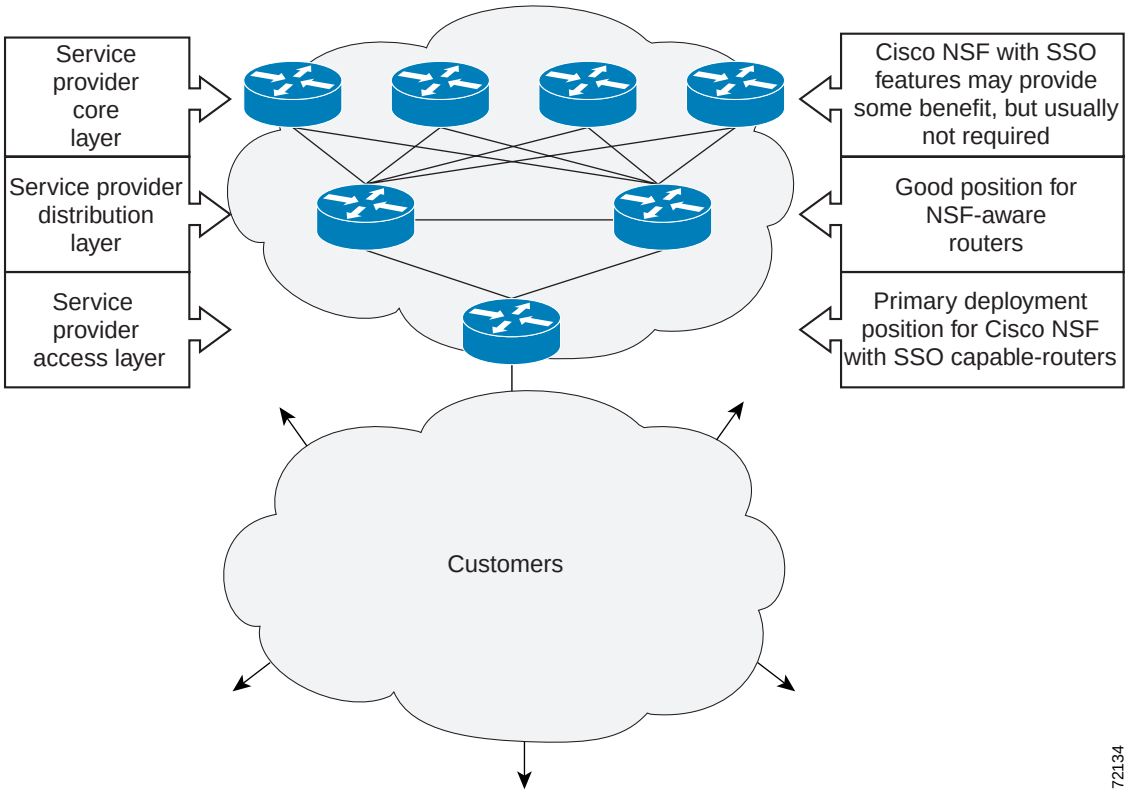
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

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

Figure 1 illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is primarily at the access layer (edge) of the service provider network. A fault at this point could result in loss of service for enterprise customers requiring access to the service provider network.

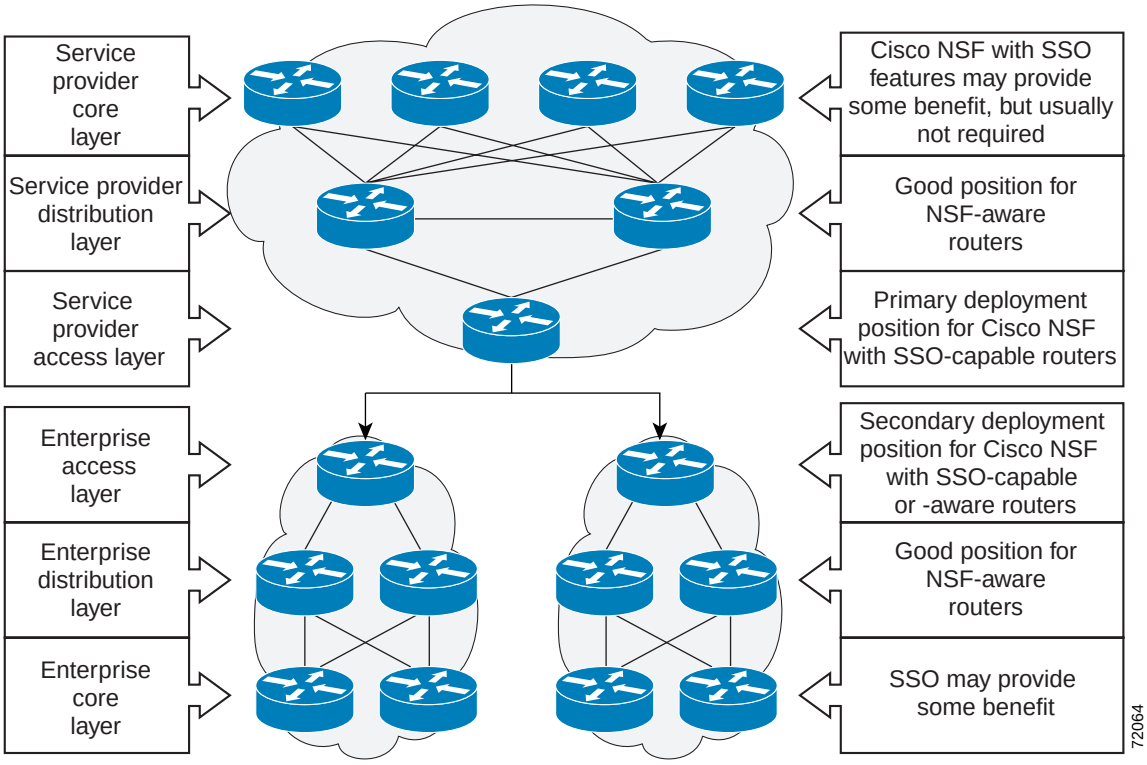
For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Additional network availability benefits might be achieved by applying Cisco NSF and SSO features at the core layer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

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



Additional levels of availability may be gained by deploying Cisco NSF with SSO at other points in the network where a single point of failure exists. Figure 2 illustrates an optional deployment strategy that applies Cisco NSF with SSO at the enterprise network access layer. In this example, each access point in the enterprise network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

Figure 2 Cisco NSF with SSO Network Deployment: Enterprise Networks



Redundancy Modes

SSO is one link in a chain of Cisco IOS redundancy features designed to provide progressively higher system and network availability. The specific configuration running on the networking device identifies Cisco IOS redundancy modes, which are described in the following sections:

- High System Availability
- Route Processor Redundancy
- Route Processor Redundancy Plus
- Stateful Switchover

Understanding the various modes is helpful in configuring and verifying SSO. Table 1 indicates which redundancy modes are supported on various platforms and releases.

High System Availability

High system availability (HSA) mode allows you to install two RPs in a single router to improve system availability. This mode is available only on Cisco 7500 series routers. Supporting two RPs in a router provides the most basic level of increased system availability through a “cold restart” feature. A cold restart means that when one RP fails, the other RP reboots the router. Thus, the router is never in a failed state for very long, thereby increasing system availability.

Route Processor Redundancy

Router Processor Redundancy (RPR) is an alternative mode to HSA and allows Cisco IOS software to be booted on the standby processor prior to switchover (a “cold boot”). In RPR, the standby RP loads a Cisco IOS 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 Redundancy Plus

In RPR+ mode, the standby RP is fully initialized. The active RP dynamically synchronizes startup and the running configuration changes to standby RP, meaning that the standby RP need not be reloaded and reinitialized (a “hot boot”). Additionally, on the Cisco 10000 and 12000 series Internet routers, the line cards are not reset in RPR+ mode. This functionality provides a much faster switchover between the processors. Information synchronized to the standby RP includes running configuration information, startup information on the Cisco 10000 and 12000 series Internet routers, and changes to the chassis state such as online insertion and removal (OIR) of hardware. Line card, protocol, and application state information is not synchronized to the standby RP.

Note On Cisco 7500 series devices, legacy IPs will default to RPR mode and must be reloaded. If three or more legacy IPs are present, then all the line cards, including the VIPs, must be reloaded.

Stateful Switchover

SSO mode provides all the functionality of RPR+ in that Cisco IOS software is fully initialized on the standby RP. In addition, SSO supports synchronization of line card, protocol, and application state information between RPs for supported features and protocols (a “hot standby”).

Note During normal operation, SSO is the only supported mode for the Cisco 10000 series Internet routers.

Table 1 Redundancy Modes by Platform and Release

Platform	Mode	Redundancy Mode Support in Cisco IOS Software Releases			
		12.0(16)ST	12.0(17)ST	12.0(19)ST	12.0(22)S
7500	HSA	Yes	Yes	Yes	Yes
	RPR	Yes	Yes	Yes	Yes
	RPR+	No	No	Yes	Yes
	SSO	No	No	No	Yes
10000	HSA	No	No	No	No
	RPR	No	No	No	No
	RPR+	Yes	Yes	Yes	Yes
	SSO	No	No	No	Yes

Table 1 Redundancy Modes by Platform and Release

Platform	Mode	Redundancy Mode Support in Cisco IOS Software Releases			
		12.0(16)ST	12.0(17)ST	12.0(19)ST	12.0(22)S
12000	HSA	No	No	No	No
	RPR	Yes	Yes	Yes	Yes
	RPR+	No	Yes	Yes	Yes
	SSO	No	No	No	Yes

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.

Note 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.

Note On Cisco 12000 series devices with three or more RPs in a chassis, after negotiation of active and standby RP, the non-active (remaining) RPs do not participate in router operation.

Synchronization of Startup Configuration

Note During system startup on Cisco 10000 and 12000 series devices, 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:

- CLI command **copy system:running-config nvram:startup-config** is used.
- CLI command **copy running-config startup-config** is used.
- CLI command **write memory** is used.
- CLI 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 CLI 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 CLI commands or Simple Network Management Protocol [SNMP]) or other internal events.

CLI Commands

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

SNMP SET Commands

Configuration changes caused by an SNMP set operation are synchronized on a case-by-case basis. Currently 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

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

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.
- For the Cisco 12000 and 7500 series routers, changes to the chassis state due to configuration changes to the alarm card or power supply cards are *not* synchronized to the standby RP. The standby RP learns these configuration changes using a discovery and reconciliation process during a switchover.

Line Card State

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.

Counters and Statistics

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.

Note Not synchronizing counters and statistics between RPs may create problems for external network management systems that monitor this information. For more information on SSO MIBs, see the "Related Documents" section of this document.

Switchover Operation

During switchover, system control and routing protocol execution are transferred from the active to the standby RP. Switchover may be due to a manual operation (CLI-invoked) or to a software- or hardware-initiated operation (hardware or software fault induced).

The following sections describe switchover operation considerations:

- Switchover Conditions
- Switchover Time
- Online Removal of the active RP
- Single Line Card Reload
- Fast Software Upgrade
- Core Dump Operation
- Core Dump 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 CLI is invoked—manual switchover

The user can force the switchover from the active RP to the dual 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:

- On the Cisco 7500 series devices, switchover time is approximately 30 seconds longer than on the Cisco 10000 series or Cisco 12000 series devices.
- On the Cisco 10000 series devices, switchover time is only a few seconds.
- On the Cisco 12000 series devices, switchover time due to a manual switchover or due to automatic switchover caused by an error is only a few seconds. If the switchover is caused by a fault on the active RP, the standby RP will detect the problem following the switchover timeout period, which is set to three seconds by default.

Whenever an SSO switchover occurs, the processor will not completely be booted up and configured in it's new state for approximately 7 minutes. The actual time of the switchover is dependant upon configuration and various other factors, and will take at least 5 minutes and 30 seconds in the best possible switchover scenario.

The following table provides some rough estimates regarding the time required to switch a new packet and total switchover time for various High Availability redundancy features:

Feature	Time to Immediately Switch a Packet on New RSP After Failover	Expected Overall Time to Have New RSP in New High Availablity State After Failover	Notes
High System Availability (HSA)	10 minutes	20 minutes	System default.
RPR	5 minutes	15 minutes	VIPs and legacy interface processors supported.
RPR+	30 seconds	11 minutes	VIPs supported.[1]
Stateful Swithover	7 seconds	7 minutes	

1. Legacy interface processors default to RPR. A message similar to the following is displayed during switchover:

```
%HA-2-NO_Quiesce: Slot 11 did not quiesce, it will be disabled and then reloaded.
```

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.

The impact of the switchover time on packet forwarding depends on the networking device:

- On the Cisco 7500 series devices, forwarding information is distributed, and packets forwarded from the same line card should see little to no forwarding delay; however, forwarding packets between line cards requires interaction with the RP, meaning that packet forwarding might have to wait for the switchover time. The switchover time on Cisco 7500 series devices is also dependent on the type of RSPs installed on the system.
- On the Cisco 10000 series devices, CEF information resides on the RP, so packet forwarding can be impacted momentarily while the switchover occurs.
- On the Cisco 12000 series devices, complete forwarding information is distributed to the line cards, so packet forwarding is not impacted as long as the line cards are working.

Online Removal of the active RP

For Cisco 7500 series routers, online removal of the active RSP will automatically switch the redundancy mode to RPR. Online removal of the active RSP causes all line cards to reset and reload, which is equivalent to an RPR switchover, and results in a longer switchover time. When it is necessary to remove the active RP from the system, first issue a switchover command to switch from the active RSP to the standby RSP. When a switchover is forced to the standby RSP before the previously active RSP is removed, the network operation benefits from the continuous forwarding capability of SSO.

For Cisco 10000 and 12000 series Internet routers that are configured to use SSO, online removal of the active RP automatically forces a stateful switchover to the standby RP.

Single Line Card Reload

In Cisco 7500 series routers, a line card might fail to reach the quiescent state as a result of a hardware or software fault. In such cases, the failing line card must be reset. We recommend using the Single Line Card Reload (SLCR) feature to provide maximum assurance that SSO will continue forwarding packets on unaffected interfaces during switchover.

Note SLCR is not required on the Cisco 10000 and 12000 series Internet routers.

The SLCR feature allows users to correct a line card fault on a Cisco 7500 series router by automatically reloading the microcode on a failed line card. During the SLCR process, all physical lines and routing protocols on the other line cards of the network backplane remain active.

The SLCR feature is not enabled by default. When you enable SSO, RPR+, or RPR, it is important that you enable SLCR also. For information on how to load and configure SLCR, refer to the *Cisco 7500 Single Line Card Reload* feature module.

Fast Software Upgrade

You can use Fast Software Upgrade (FSU) to reduce planned downtime. With FSU, you can configure the system to switch over to a standby RP that is preloaded with an upgraded Cisco IOS software image. FSU reduces outage time during a software upgrade by transferring functions to the standby RP that has the upgraded Cisco IOS software preinstalled. You can also use FSU to downgrade a system to an older version of Cisco OS or have a backup system loaded for downgrading to a previous image immediately after an upgrade.

Note During the upgrade process, different images will be loaded on the RPs for a short period of time. During this time, the device will operate in RPR or RPR+ mode, depending on the networking device.

Core Dump Operation

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

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

The core dump process adds the slot number to the core dump file to identify which processor generated the file content. For more information on how to complete a core dump, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2.

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

SSO-Aware Protocols and Applications

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

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

SSO-aware applications are either platform-independent, such as in the case of line protocols (Frame Relay, ATM, and PPP) or platform-dependent (such as line card drivers). Enhancements to the routing protocols (CEF, 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.

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

- ATM Stateful Switchover
- Frame Relay Stateful Switchover
- PPP and Multilink PPP Stateful Switchover
- HDLC Stateful Switchover

Table 2 indicates which protocols are supported on various platforms and releases.

Table 2 Line Protocol Support in SSO

Protocol	Platform	Cisco IOS Software Release 12.0(22)S
ATM	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes
Frame Relay	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	No
PPP and Multilink PPP	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes

Table 2 Line Protocol Support in SSO (continued)

Protocol	Platform	Cisco IOS Software Release 12.0(22)S
HDLC	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes

ATM Stateful Switchover

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

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

Permanent Virtual Circuits

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

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

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

ATM OAM Managed PVC or SVC Timeout

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

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

Frame Relay Stateful Switchover

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

Permanent Virtual Circuits

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

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

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

Keepalive Messages

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

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

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

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

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

If a line goes down, consecutive successful LMI protocol exchanges (default of four over 40 seconds on a Cisco Frame Relay switch; default of two over 20 seconds on a Cisco IOS 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.

Line Card Drivers

Platform-specific line card device drivers are bundled with the Cisco IOS 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.
- 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.

For a list of supported line cards, see the "Restrictions" section of this document.

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 (dual forwarding processors (FPs) on Cisco 10000 series Internet routers) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards (and FPs on Cisco 10000 series devices) 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 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 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 CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables.

For more information on Cisco NSF, see the "Related Documents" section of this document.

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.

For more information on SNMP support for SSO, see the "Related Documents" section of this document.

Benefits

Improved Network Availability

Because SSO maintains protocol and application state information, user session information is maintained after a switchover, meaning that line cards continue to forward network traffic with no loss of sessions.

Improved Switchover Time

SSO provides a faster switchover relative to HSA, RPR, and RPR+ by fully initializing and fully configuring the standby RP, and by synchronizing state information, which can reduce the time required for routing protocols to converge.

Improved Network Stability

Network stability may be improved with the reduction in the number of route flaps had been created when routers in the network failed and lost their routing tables.

Restrictions

General Restrictions for SSO

- Both RPs must run the same Cisco IOS image. If the RPs are operating different Cisco IOS images, the system reverts to RPR mode even if SSO is configured. On the Cisco 10000 series Internet router, the system reverts to RPR+ mode.
- For Cisco NSF support, neighbor routers need to be running Cisco NSF-enabled images, though SSO need not be configured on the neighbor device.
- Configuration changes made through SNMP may not be automatically configured on the standby RP after a switchover occurs.
- Load sharing between dual processors is not supported.
- Multicast is not SSO-aware and restarts after switchover; therefore, multicast tables and data structures are cleared upon switchover.
- Multiprotocol Label Switching (MPLS) does not support SSO in the current release. MPLS is not SSO-aware and restarts after switchover; therefore, MPLS tables and data structures are cleared upon switchover.
- Label-controlled ATM (LC-ATM) functionality does not co-exist with SSO in this release.

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.
```

Switchover Process Restrictions

- On the Cisco 12000 and 7500 series routers, if any changes to the fabric configuration happen simultaneously with an RP switchover, the chassis is reset and all line cards are downloaded.
- If a switchover occurs before the standby RP is fully initialized, the chassis is reset and will not switch over in RPR mode.
- On Cisco 7500 series routers configured for SSO mode, during synchronization between the active and standby RPs, the configured mode will be RPR. After the synchronization is complete, the operating mode will be SSO. If a switchover occurs before the synchronization is complete, the switchover will be in RPR mode.
- On the Cisco 12000 series and 10000 series Internet routers, if a switchover occurs before the bulk synchronization step is complete, the new active RP may be in inconsistent states. The router will be reloaded in this case.

ATM Restrictions

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

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 using a CLI command. 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.

PPP Restrictions

- The following PPP features are not supported in this release: dialer; authentication, authorization, and accounting (AAA), IPPOOL, Dynamic Host Configuration Protocol (DHCP), Layer 2 (L2X), Point-to-Point Tunneling Protocol (PPTP), Microsoft Point-to-point Encryption (MPPE), Point-to-Point Protocol over Ethernet (PPPoE), Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA), Link Quality Monitoring (LQM), link or header compression, bridging, asynchronous PPP, and XXCP.
- We recommend that the keepalive value be set to 20 seconds on Cisco 7500 series routers for each peer in a PPP connection.

Cisco 12000 Series Internet Router Platform Restrictions

- Any line cards that are not online at the time of a switchover (line cards not in Cisco IOS running state) are reset and reloaded on a switchover.
- The following line cards support SSO and Cisco NSF:
  - All Engine-0, Engine-2, and Engine-4 Packet over SONET (PoS) line cards
  - All Engine-0 ATM line cards
  - All nonchannelized DS3 and E3 line cards
  - All Engine-0 channelized line cards
- The following Engine-0 line cards are supported:
  - 4-port OC-3 POS

  - 1-port OC-12 POS
  - 1-port O-12 ATM
  - 4-port OC-3 ATM
  - 6-port DS3
  - 12-port DS3
  - 6-port E3
  - 12-port E3
  - 6-port CT3
  - 1-port CHOC-12->DS3
  - 6-port CT3->DS1
  - 1-port CHOC-12/STM4->OC-3/STM1 POS
  - 2-port CHOC-3/STM-1->DS1/E1
- The following Engine-2 line cards are supported:
  - 1-port OC-48 POS
  - 4-port OC-12 POS
  - 8-port OC-3 POS
  - 16-port OC-3 POS
- The following Engine-4 line cards are supported:
  - 1-port OC-192 POS
  - 4-port OC-48 POS

Cisco 10000 Series Internet Router Platform Restrictions

- The following line cards support SSO and Cisco NSF:
  - 6-port Universal (Channelized or Clear-channel) DS3
  - 8-port E3/DS3
  - 1-port OC-12 POS
  - 6-port OC-3 POS
  - 1-port Gigabit Ethernet
  - 1-port Channelized OC-12
  - 4-port Channelized STM1
  - 24-port channelized E1/T1
  - 1-port OC-12 ATM
  - 4-port OC-3 ATM

Cisco 7500 Series Internet Router Platform Restrictions

- SSO operates only on a Cisco 7500 series Internet router that has VIPs as the line cards. Systems with legacy interface processors not compatible with RPR+ or SSO mode will always get reset and reloaded upon switchover.

- To support SSO, a router must have either two RSP8 devices, or any combination of RSP2 and RSP4 on the Cisco 7513 and 7507 platforms. A combination of RSP8 with RSP2 or RSP4 devices on a platform is not supported.
- Simultaneous changes to the configuration from multiple CLI sessions is not allowed. Only one configuration session is allowed to enter into configuration mode at a time: Other sessions will not be able to enter into configuration mode.
- Using "send break" to break or pause the system is not recommended and may cause unpredictable results. To initiate a manual switchover, use the **redundancy force-switchover** command.
- The following line cards support SSO and Cisco NSF:
  -
  - PA-MC-E3, 1-port multichannel E3 port adapter (PA)
  - PA-MC-T3, 1-port multichannel T3 PA
  - PA-MC-2E1/120, 2-port multichannel E1 PA with G.703 120-ohm interface
  - PA-MC-2TE1, 2-port multichannel T1 PA with integrated channel service unit (CSU) and data service unit (DSU) devices
  - PA-MC-2T3+, 2-port multichannel T3 PA
  - PA-MC-4T, 4-port multichannel T1 PA with integrated CSU and DSU devices
  - PA-MC-8T1, 8-port multichannel T1 PA with integrated CSU and DSU devices
  - PA-MC-8DSX1, 8-port multichannel DS1 PA with integrated DSUs
  - PA-MC-8E1/120, 8-port multichannel E1 PA with G.703 120-ohm interface
  - PA-2T3, 2-port T3 serial PA
  - PA-4T+, 4-port serial PA enhanced
  - PA-8T-V35, 8-port serial V.35 PA
  - PA-8T-232, 8-port serial 232 PA
  - PA-8T-X21, 8-port serial X.21 PA
  - PA-E3, 1-port E3 serial PA with E3 DSU
  - PA-T3+, 1-port T3 serial PA enhanced
  - PA-2E3, 2-port E3 serial PA with E3 DSUs
  - PA-2T3+, 2-port T3 serial PA enhanced
  - PA-H, 1-port High-Speed Serial Interface (HSSI) PA
  - PA-2H, 2-port HSSI PA
  - PA-2FE-TX, 2-port Ethernet 100BASE-TX PA
  - PA-2FE-FX, 2-port Ethernet 100BASE-FX PA
  - PA-FE-TX, 1-port Fast Ethernet 100BASE-TX PA
  - PA-FE-FX, 1-port Fast Ethernet 100BASE-FX PA
  - PA-4E 4-port, Ethernet 10BASE-T PA
  - PA-8E 8-port, Ethernet 10BASE-T PA
  - PA-A3-E3, 1-port ATM enhanced E3 PA
  - PA-A3-T3, 1-port ATM enhanced DS3 PA

  - PA-A3-OC3MM, 1-port ATM enhanced OC-3c/STM-1 multimode PA
  - PA-A3-OC3SMI, 1-port ATM enhanced OC-3c/STM-1 single-mode (IR) PA
  - PA-A3-OC3SML, 1-port ATM enhanced OC-3c/STM-1 single-model (LR) PA
  - PA-POS-OC3MM, 1-port PoS OC-3c/STM-1 multimode PA
  - PA-POS-OC3SMI, 1-port PoS OC-3c/STM-1 single-mode (IR) PA
  - PA-POS-OC3SML, 1-port PoS OC-3c/STM-1 single-mode (LR) PA
  - PA-A3-8E1IMA, 8-port ATM inverse multiplexer E1 (120-ohm) PA
  - PA-A3-8T1IMA, 8-port ATM inverse multiplexer T1 PA
  - PA-4E1G/75, 4-port E1 G.703 serial PA (75-ohm/unbalanced)
  - PA-4E1G/120, 4-port E1 G.703 serial PA (120-ohm/balanced)
  - PA-MCX-8TE1
  - PA-MCX-4TE1
  - PA-MCX-2TE1
  - PA/VIP Combinations:
- Gigabit-Ethernet IP (GEIP)
- GEIP+

Related Features and Technologies

- RPR+
- NSF

Related Documents

- *Route Processor Redundancy Plus for the Cisco 12000 Series Internet Routers*, Cisco IOS Release 12.0(17)ST feature module
- *RPR+ on Cisco 7500 Series Routers*, Cisco IOS Release 12.0(17)ST feature module
- *Cisco Nonstop Forwarding*, Cisco IOS Release 12.0(22)S feature module
- *SNMP for Stateful Switchover*, Cisco IOS Release 12.0(22)S feature module
- *Cisco 7500 Single Line Card Reload*, Cisco IOS Release 12.0(13)S feature module

Supported Platforms

The SSO feature is supported on the following platforms:

- Cisco 7500 series
- Cisco 10000 series
- Cisco 12000 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- Two (dual) RPs must be installed in the chassis, each running the same version of the Cisco IOS software.
- On the Cisco 7513 and 7507 platforms, two RSP8 devices, or any combination of RSP2 and RSP4, are required.
- Distributed CEF must be enabled on any networking device configured to run SSO. Configure distributed CEF (dCEF) on Cisco 7500 series routers using the **ip cef distributed** global configuration command. Distributed CEF is enabled by default on Cisco 12000 and 10000 series Internet routers.
- SSO supports TFTP boot operation only on the Cisco 10000 series Internet routers. For other platforms, the software images must be downloaded to the Flash memory cards on the router.

Configuration Tasks

See the following sections for configuration tasks for the SSO feature. Each task in the list is identified as either required or optional.

- Copying an Image onto an RP (required)
- Setting the Configuration Register and Boot Variable (required)
- Configuring SSO (required)
- Configuring Frame Relay Autosynchronization LMI Sequence Numbers (Optional)
- Verifying SSO (optional)
- Performing a Fast Software Upgrade (optional)

Copying an Image onto an RP

To copy a Cisco IOS image onto the active and standby RP devices using TFTP, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# copy tftp slot`*slot-number*`:`*image* or `Router# copy tftp disk`*disk-number*`:`*image*	Uses TFTP to copy a Cisco IOS image onto the Flash device of the active RP.[1]
Step 2	For Cisco 7500 series networking devices: `Router# copy tftp slaveslot`*slot-number*`:`*image* or `Router# copy tftp slavedisk`*disk-number*`:`*image* For other Cisco devices: `Router# copy tftp stby-slot`*slot-number*`:`*image* or `Router# copy tftp stby-disk`*disk-number*`:`*image*	Uses TFTP to copy a Cisco IOS image onto the Flash device of the standby RSP.

1. Before you copy 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).`

Setting the Configuration Register and Boot Variable

Note On Cisco 10000 series devices, to boot both Performance Routing Engines (PREs) from the TFTP boot server, you must enable DHCP on the PRE using the **ip address negotiated** command in interface configuration mode. Otherwise, you will get a duplicate IP address error because of the synchronization of the IP address from the active to the standby RP. Booting from the TFTP boot server is not supported on other platforms.

To set the boot image file and to modify the software configuration register boot field so that the system boots the proper image, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# show version`	Obtains the current configuration register setting.
Step 2	`Router# configure terminal`	Enters global configuration mode, selecting the terminal option.

	Command	Purpose

Step 3	`Router(config)# no boot system flash [flash-fs:][partition-number:][filename]`
	
	or
	
	`Router(config)# no boot system tftp filename [ip-address]`
		(Optional) Clears any existing system Flash or TFTP boot image specification.

Step 4	`Router(config)# boot system flash [flash-fs:][partition-number:][filename]`
	
	For the Cisco 10000 series only:
	
	`Router(config)# boot system tftp filename [ip-address]`
		Specifies the filename of an image stored in Flash memory or on a TFTP server.
		
		The Cisco 10000 series Internet router is the only networking device capable of being configured to boot from a TFTP server.

Step 5	`Router(config)# config-register value`	Modifies the existing configuration register setting to reflect the way in which you want to load a system image. • *value*—0x0 to 0xFFFFFFFF.
Step 6	`Router(config)# exit`	Exits configuration mode and returns the router to privileged EXEC mode.
Step 7	`Router# copy running-config startup-config`	Saves the configuration changes to the startup configuration file.
Step 8	`Router# reload`	Reboots both RPs on the device to ensure that changes to the configuration take effect. •

Following the reload, each RP is in it's default mode:

- The Cisco 7500 series router reboots in HSA mode.
- The Cisco 10000 series Internet router reboots in SSO mode.
- The Cisco 12000 series Internet router reboots in RPR mod.

Configuring SSO

Note Cisco 10000 series Internet routers operate in SSO mode by default after reloading the same version of SSO-aware images on the device. No configuration is necessary.

To configure SSO, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	Perform this step on Cisco 7500 series devices only: `Router(config)# hw-module slot` *slot-number* `image` *file-sp*	Specifies the image to be used by the active RSP at initialization. If a high-availability image is found, the running configuration is updated. • *slot-number*—Specifies the standby RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. • *file-spec*—Indicates the Flash device and the name of the image on the standby RSP. **Note** Step 2 and Step 3 are the same. Step 2 applies to the active RSP, and Step 3 applies to the standby RSP. If you do not specify a Cisco IOS image in Step 2, this command loads and executes the bundled default Cisco IOS standby image. The system then operates in HSA mode. The image indicated by the *file-spec* attribute must be available on the local Flash device. Remote protocols such a TFTP and remote copy are not available.
Step 3	Perform this step on Cisco 7500 series devices only: `Router(config)# hw-module slot` *slot-number* `image` *file-spec*	Specifies the image to be used by the standby RSP at initialization. If a high-availability image is found, the running configuration is updated. • *slot-number*—Specifies the active RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. • *file-spec*—Indicates the Flash device and the name of the image on the active RSP. **Note** Step 2 and Step 3 are the same. Step 2 applies to the active RSP, and Step 3 applies to the standby RSP. The image indicated by the *file-spec* attribute must be available on the local Flash device. Remote protocols such a TFTP and rcp are not available.

	Command	Purpose
Step 4	`Router(config)# redundancy`	Enters redundancy configuration mode.
Step 5	`Router(config-red)# 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 6	`Router(config-red)# end`	Exits redundancy configuration mode and returns the router to EXEC mode.
Step 7	`Router# copy running-config startup-config`	Saves the configuration changes to the startup configuration file.

Configuring Frame Relay Autosynchronization LMI Sequence Numbers

To configure Frame Relay SSO to synchronize LMI sequence numbers between the active and standby RPs, use the following command in global configuration mode. This procedure is only for devices supporting Frame Relay and is optional.

Command	Purpose
`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

To verify that SSO is configured on the networking device, use the **show redundancy** command. To verify that the device is running in SSO mode, use the **show redundancy states** command. The **show redundancy states** command specifies whether the unit is running in SSO mode, which is indicated by STANDBY HOT.

Note The output of these commands will vary based on your device configuration and system site requirements.

Step 1 Enter the **show redundancy** command to verify that SSO is configured on the device. Sample output is provided for the various platforms:

Cisco 7500 Series

```
Router# show redundancy

Operating mode is sso
redundancy mode sso
hw-module slot 6 image disk0:rsp-pv-mz
hw-module slot 7 image disk0:rsp-pv-mz

Active in slot 6
Standby in slot 7

The system total uptime since last reboot is 2 weeks, 23 hours 41 minutes.
The system has experienced 4 switchovers.
```

```
The system has been active (become master) for 21 hours 1 minute.
Reason for last switchover: User forced.
```

Cisco 10000 Series Internet Router

```
Router# show redundancy

PRE A (This PRE)   : Active
PRE B              : Standby

Operating mode                : SSO
Uptime since this PRE switched to active : 13 hours, 51 minutes
Total system uptime from reload      : 15 hours, 8 minutes
Switchovers this system has experienced : 2
Standby failures since this PRE active  : 0
The standby PRE has been up for    : 13 hours, 47 minutes

Standby PRE information....
Standby is up.
Standby has 524288K bytes of memory.
Standby BOOT variable = disk0:c10k-p10-mz
Standby CONFIG_FILE variable =
Standby BOOTLDR variable =
Standby Configuration register is 0x2102

Standby version:
Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (C10K-P10-M), Experimental Version 12.0(20020221:082811)
 [REL-bowmore.ios-weekly 100]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 21-Feb-02 03:28

Active version:
Cisco Internetwork Operating System Software
IOS (am) 10000 Software (C10K-P10-M), Experimental Version 12.0(20020221:082811)
 [REL-bowmore.ios-weekly 100]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 21-Feb-02 03:28
```

Cisco 12000 Series Internet Router

```
Router# show redundancy
Active GRP in slot 4:
Standby GRP in slot 5:
Preferred GRP:  none
Operating Redundancy Mode: SSO
Auto synch: startup-config running-config
switchover timer 3 seconds [default]
```

Step 2 Run the **show redundancy states** command to verify that SSO is operating on the device. Sample output is provided for the various platforms:

Cisco 7500 Series Router

```
Router# show redundancy states

my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit ID = 7

Redundancy Mode = sso
Maintenance Mode = Disabled
Manual Swact = Enabled
```

```
Communications = Up

client count = 12
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
```

Cisco 10000 Series Internet Router

```
Router# show redundancy states

my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit = Preferred Primary
Unit ID = 0

Redundancy Mode = SSO
Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up

client count = 14
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
```

Cisco 12000 Series Internet Router

```
Router# show redundancy states

my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit ID = 4

Redundancy Mode = SSO
Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up

client count = 14
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x
```

Step 3 Enter the **show redundancy client** command to display the list of applications and protocols that have registered as SSO protocols or applications. Verify the list of supported line protocols.

Cisco 7500 Series Router

```
Router# show redundancy client

 clientID = 0      clientSeq = 0        RF_INTERNAL_MSG
 clientID = 25     clientSeq = 130      CHKPT RF
 clientID = 22     clientSeq = 140      Network RF Client
 clientID = 24     clientSeq = 150      CEF RRP RF Client
 clientID = 37     clientSeq = 151      MDFS RRP RF Client
 clientID = 23     clientSeq = 220      FRAME RELAY
 clientID = 49     clientSeq = 225      HDLC
 clientID = 20     clientSeq = 310      IPROUTING NSF RF cli
 clientID = 21     clientSeq = 320      PPP RF
 clientID = 34     clientSeq = 330      SNMP RF Client
 clientID = 29     clientSeq = 340      ATM
 clientID = 35     clientSeq = 350      History RF Client
 clientID = 50     clientSeq = 530      SNMP HA RF Client
```

```
 clientID = 65000  clientSeq = 65000    RF_LAST_CLIENT
```

Cisco 10000 Series Internet Router

```
Router# show redundancy client

 clientID = 0      clientSeq = 0        RF_INTERNAL_MSG
 clientID = 25     clientSeq = 130      CHKPT RF
 clientID = 22     clientSeq = 140      Network RF Client
 clientID = 24     clientSeq = 150      CEF RRP RF Client
 clientID = 26     clientSeq = 160      C10K RF Client
 clientID = 5      clientSeq = 170      RFS client
 clientID = 23     clientSeq = 220      Frame Relay
 clientID = 49     clientSeq = 225      HDLC
 clientID = 20     clientSeq = 310      IPROUTING NSF RF cli
 clientID = 21     clientSeq = 320      PPP RF
 clientID = 34     clientSeq = 330      SNMP RF Client
 clientID = 29     clientSeq = 340      ATM
 clientID = 35     clientSeq = 350      History RF Client
 clientID = 65000  clientSeq = 65000    RF_LAST_CLIENT
```

Cisco 12000 Series Internet Router

```
Router# show redundancy client

clientID = 0      clientSeq = 0        RF_INTERNAL_MSG
 clientID = 25     clientSeq = 130      CHKPT RF
 clientID = 27     clientSeq = 132      C12K RF COMMON Clien
 clientID = 30     clientSeq = 135      Redundancy Mode RF
 clientID = 22     clientSeq = 140      Network RF Client
 clientID = 24     clientSeq = 150      CEF RRP RF Client
 clientID = 37     clientSeq = 151      MDFS RRP RF Client
 clientID = 5      clientSeq = 170      RFS client
 clientID = 23     clientSeq = 220      Frame Relay
 clientID = 49     clientSeq = 225      HDLC
 clientID = 20     clientSeq = 310      IPROUTING NSF RF cli
 clientID = 21     clientSeq = 320      PPP RF
 clientID = 34     clientSeq = 330      SNMP RF Client
 clientID = 29     clientSeq = 340      ATM
 clientID = 35     clientSeq = 350      History RF Client
 clientID = 50     clientSeq = 530      SNMP HA RF Client
 clientID = 65000  clientSeq = 65000    RF_LAST_CLIENT
```

Performing a Fast Software Upgrade

The FSU procedure allows you to upgrade (or downgrade) the Cisco IOS image on the RPs. To perform an FSU, use the following commands beginning in privileged EXEC mode.

Cisco IOS software is upgraded on the standby RP, and a manual switchover is performed. The new Cisco IOS image can then be upgraded on the other RPs.

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

This procedures assumes that SSO previously has been configured on the networking device.

	Command	Purpose
Step 1	`Router# copy tftp slot`*slot-number*`:`*image* or `Router# copy tftp disk`*disk-number*`:`*image*	Uses TFTP to copy a high-availability Cisco IOS image onto the Flash device of the active RP.[1]
Step 2	For Cisco 7500 series networking devices: `Router# copy tftp slaveslot`*slot-number*`:`*image* or `Router# copy tftp slavedisk`*disk-number*`:`*image* For other Cisco devices: `Router# copy tftp stby-slot`*slot-number*`:`*image* or `Router# copy tftp stby-disk`*disk-number*`:`*image*	Uses TFTP to copy a high-availability Cisco IOS image onto the Flash device of the standby RSP.
Step 3	`Router# configure terminal`	Enters global configuration mode.
Step 4	Perform this step on the Cisco 7500 only: `Router(config)# no hw-module slot` *slot-number* `image` *file-spec*	Clears existing configuration entries for the specified image on the standby RSP. Configuration entries are additive, and the networking device will use the first image found in the configuration file. • *slot-number*—Specifies the standby processor slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. • *file-spec*—Indicates the Flash device and the name of the image on the standby processor.
Step 5	Perform this step on the Cisco 7500 only: `Router(config)# no hw-module slot` *slot-number* `image` *file-spec*	Clears existing configuration entries for the specified image on the active RSP. Configuration entries are additive, and the networking device will use the first image found in the configuration file. • *slot-number*—Specifies the active RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. • *file-spec*—Indicates the Flash device and the name of the image of the active processor.

	Command	Purpose
Step 6	Perform this step on the Cisco 7500 only: `Router(config)# hw-module slot slot-number image file-spec`	Specifies the image to be used by the standby RSP at initialization. If a high-availability image is found, the running configuration is updated. • *slot-number*—Specifies the standby RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. • *file-spec*—Indicates the Flash device and the name of the image on the standby processor.
Step 7	Perform this step on the Cisco 7500 only: `Router(config)# hw-module slot slot-number image file-spec`	Specifies the image to be used by the active RSP at initialization. If a high-availability image is found, the running configuration is updated. • *slot-number*—Specifies the active RSP slot where the Flash memory card is located. Valid numbers are slot 2 or slot 3 for a Cisco 7507 router or slot 6 or slot 7 for a Cisco 7513 router. • *file-spec*—Indicates the Flash device and the name of the image of the active processor.
Step 8	`Router(config)# no boot system flash [flash-fs:][partition-number:][filename]`	Clears the current boot image filename from the configuration file.
Step 9	`Router(config)# boot system flash [flash-fs:][partition-number:][filename]`	Specifies the filename of a boot image stored in Flash memory as in Step 2.
Step 10	`Router(config)# config-register value`	Modifies the existing configuration register setting to reflect the way in which you want to load a system image. • *value*—0x2 to 0xFFFFFFFF.
Step 11	`Router(config)# exit`	Exits configuration mode and returns the router to privileged EXEC mode.
Step 12	`Router# copy running-config startup-config`	Saves the configuration changes to your startup configuration in NVRAM so that the router will boot with the configuration you have entered.

Step 13	For Cisco 12000 series networking devices:
	`Router# reload standby-cpu`
	For other networking devices:
	`Router# hw-module standby-cpu reset`
		Resets and reloads the standby processor with the specified Cisco IOS image, and executes the image.
		Note If you do not specify a Cisco IOS image in Step 9, this command loads and executes the bundled default Cisco IOS standby image.

Step 14	For Cisco 10000 series networking devices:
	`Router# redundancy force-switchover main-cpu`
	For other networking devices:
	`Router# redundancy force-switchover`
		Forces a switchover to the standby RP.

1. Before you copy 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).`

Troubleshooting Tips

To troubleshoot the SSO feature, use the following commands in redundancy or EXEC mode, as needed:

Command	Purpose
`router(config-r)# crashdump-timeout`	Set the longest time that the newly active Route Switch Processor (RSP) will wait before reloading the formerly active RSP.
`Router# debug atm ha-errors`	Debugs ATM high-availability errors on the networking device.
`Router# debug atm ha-events`	Debugs ATM high-availability events on the networking device.
`Router# debug atm ha-state`	Debugs ATM high-availability state information on the networking device.
`Router# debug frame-relay redundancy`	Debugs Frame Relay redundancy on the networking device.
`Router# debug ppp redundancy`	Debugs PPP redundancy on the networking device.
`Router# debug redundancy`	Debugs redundancy on the networking device.
`Router# show diag`	Displays hardware information for the router.
`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.
`Router# show version`	Displays image information for each RP.

The following tips can help to troubleshoot SSO operation.

The standby RP was reset, but there are no messages describing what happened.

To display a log of SSO events and clues as to why a switchover or other event occurred, enter the **show redundancy history** command on the newly active RP:

```
Router# show redundancy history
```

The show redundancy states command shows an operating mode that is different than what is configured on the networking device.

On certain platforms the output of the **show redundancy states** command displays the actual operating redundancy mode running on the device, and not the configured mode as set by the platform. The operating mode of the system can change depending on system events. For example, SSO requires that both RPs on the networking device be running the same software image; if the images are different, the device will not operate in SSO mode, regardless of its configuration.

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

Note On the Cisco 10000 series Internet router, if the router images are not the same the router will recover in RPR+ mode as long as the images are SSO-capable. If both images are not SSO-capable, the router will recover in RPR mode.

Reloading the device disrupts SSO operation.

The SSO feature introduces a number of commands, including commands to manually cause a switchover. The reload command is not an SSO command. This command causes a full reload of the box, removing all table entries, resetting all line cards, and thereby interrupting network traffic forwarding. To avoid reloading the box unintentionally, use the **redundancy force-switchover** command.

During a software upgrade, the networking device appears to be in a mode other than SSO.

During the software upgrade process, the show redundancy command indicates that the device is running in a mode other than SSO.

This is normal behavior. Until the FSU procedure is complete, each RP will be running a different software version. While the RPs are running different software versions, the mode will change to either RPR or RPR+, depending on the device. The device will change to SSO mode once the upgrade has completed.

On the Cisco 7500 series router, the previously active processor is being reset and reloaded before the core dump completes.

Use the **crashdump-timeout** command to set the maximum time that the newly active processor waits before resetting and reloading the previously active processor.

On the Cisco 7500 series router, issuing a "send break" does not cause a system switchover.

This is normal operation on the Cisco 7500 series router. Using "send break" to break or pause the system is not recommended and may cause unpredictable results. To initiate a manual switchover, use the **redundancy force-switchover** command.

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

On Cisco 10000 and 12000 series Internet routers, if a standby RP is present, the system will detect the break and complete a switchover; however, this is not the recommended procedure for initiating a switchover. To initiate a manual switchover, use the **redundancy force-switchover** command.

Configuration Examples

This section provides the following configuration examples:

- Copying an Image onto an RP Examples
- Setting the Configuration Register Boot Variable Examples
- Configuring SSO Examples
- Configuring Autosync LMI Sequence Numbers Example

Copying an Image onto an RP Examples

The examples in this section copy an SSO-aware software image to Flash memory on each of the RPs.

This section includes the following examples:

- Copying an Image onto the Active and standby RPs on the Cisco 7500 Example
- Copying an Image onto Active and standby RPs on the Cisco 10000 Example
- Copying an Image onto Active and standby RPs on the Cisco 12000 Example

Copying an Image onto the Active and standby RPs on the Cisco 7500 Example

This example copies an SSO-aware software image to Flash memory on each of the RSPs of a Cisco 7500 series router.

```
Router# copy tftp slot0:rsp-pv-mz
Router# copy tftp slaveslot0:rsp-pv-mz
```

The system will prompt you for additional server and filename information for each **copy** command.

Copying an Image onto Active and standby RPs on the Cisco 10000 Example

This example copies an SSO-aware software image to Flash memory on each of the PREs of a Cisco 10000 series Internet router.

```
Router# copy tftp disk0:c10k-p10-mz
Router# copy tftp stby-disk0:c10k-p10-mz
```

The system will prompt you for additional server and filename information for each **copy** command.

Copying an Image onto Active and standby RPs on the Cisco 12000 Example

This example copies an SSO-aware software image to Flash memory on each GRP of a Cisco 12000 series Internet router.

```
Router# copy tftp slot0:gsr-p-mz
Router# copy tftp stby-slot0:gsr-p-mz
```

The system will prompt you for additional server and filename information for each **copy** command.

Setting the Configuration Register Boot Variable Examples

The examples in this section configure the configuration register boot variable to boot from Flash and then reload each of the RPs with the new image:

This section includes the following examples:

- Setting the Configuration Register Boot Variable on the Cisco 7500 Example
- Setting the Configuration Register Boot Variable on the Cisco 10000 Example
- Setting the Configuration Register Boot Variable on the Cisco 12000 Example

Setting the Configuration Register Boot Variable on the Cisco 7500 Example

This example sets the configuration register boot variable to boot from Flash and then reload each of the RSPs with the new image.

```
Router# show version
Router# configure terminal
Router(config)# no boot system flash slot0:
Router(config)# boot system flash slot0:rsp-pv-mz
Router(config)# config-register 0x2101
Router(config)# exit
Router# copy running-config startup-config
Router# reload
```

Setting the Configuration Register Boot Variable on the Cisco 10000 Example

This example sets the configuration register boot variable to boot from Flash and then reload each of the PREs with the new image.

```
Router# show version
Router# configure terminal
Router(config)# no boot system flash slot0:
Router(config)# boot system flash disk0:c10k-p6-mz
Router(config)# config-register 0x2101
Router(config)# exit
Router# copy running-config startup-config
Router# reload
```

Setting the Configuration Register Boot Variable on the Cisco 12000 Example

This example sets the configuration register boot variable to boot from Flash and then reload each GRP with the new image.

```
Router# show version
Router# configure terminal
Router(config)# no boot system flash slot0:
Router(config)# boot system flash slot0:gsr-p-mz
Router(config)# config-register 0x2101
Router(config)# exit
Router# copy running-config startup-config
Router# reload
```

Configuring SSO Examples

Note The Cisco 1000 series Internet router operates in SSO mode by default after reloading SSO-aware images on the device. No configuration is necessary.

This section includes the following examples:

- Configuring SSO on the Cisco 7500 Series Example
- Configuring SSO on the Cisco 12000 Series Example

Configuring SSO on the Cisco 7500 Series Example

In the following example, the active RSP is installed in slot 6 and the standby RSP is installed in slot 7 of a Cisco 7513 router:

```
Router# configure terminal
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# end
Router# copy running-config startup-config
```

Configuring SSO on the Cisco 12000 Series Example

In the following example configures SSO mode on the active RP; the standby RP is automatically reset and synchronized with the active RP.

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

Configuring Autosync LMI Sequence Numbers Example

In the following example, Frame Relay SSO is configured to support autosynchronization of LMI sequence numbers between the active RP and standby RP:

```
Router (config)# frame-relay redundancy auto-sync lmi-sequence-numbers
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS command reference publications for various releases.

New Commands

- **crashdump-timeout**
- **debug atm ha-error**
- **debug atm ha-events**
- **debug atm ha-state**
- **debug frame-relay redundancy**
- **debug ppp redundancy**
- **frame-relay redundancy auto-sync lmi-sequence-numbers**

Modified Commands

- **debug redundancy**
- **mode (redundancy)**
- **redundancy**
- **redundancy force-switchover**
- **reload**
- **show redundancy**

crashdump-timeout

To set the longest time that the newly active Route Switch Processor (RSP) will wait before reloading the formerly active RSP, use the **crashdump-timeout** command in global configuration mode. To reset the default time that newly active RSP will wait before reloading the formerly active RSP, use the **no** form of this command.

crashdump-timeout [**mm** | **hh:mm**]

no crashdump-timeout

Syntax Description

mm	(Optional) The time, in minutes, that the newly active RSP will wait before reloading the formerly active RSP. The range is from 5 to 1080 minutes.
hh:mm	(Optional) The time, in hours and minutes, that the newly active RSP will wait before reloading the formerly active RSP. The range is from 5 minutes to 18 hours.

Defaults

The default timeout for the command is 5 minutes.

Command Modes

Redundancy

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 7500 series routers.

Usage Guidelines

Use this command to specify the length of time that the newly active RSP will wait before reloading the previously active RSP. This time can be important when considering how long to wait for a core dump to complete before reloading the RSP.

In networking devices that support stateful switchover (SSO), the newly active primary processor runs the core dump operation after the switchover has taken place. Following the switchover, the newly active RSP will wait for a period of time for the core dump to complete before attempting to reload the formerly active RSP.

In the event that the core dump does not complete within the time period provided, the standby RSP is reset and reloaded based on the **crashdump timeout** command setting, regardless of whether it is still performing a core dump.

Note The core dump process adds the slot number to the core dump file to identify which processor generated the file content. For more information on how to configure the system for a core dump, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.0.

Examples

The following example sets the time before the previously active RSP is reloaded to 10 minutes:

```
router(config-r)# crashdump-timeout 10
```

debug atm ha-error

To debug ATM high-availability (HA) errors on a networking device, use the **debug atm ha-error** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug atm ha-error

no debug atm ha-error

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.

Examples

The following example displays debug messages regarding ATM HA errors on the networking device:

```
router# debug atm ha-error
```

Related Commands

Command	Description
debug atm ha-events	Debugs ATM HA events on the networking device.
debug atm ha-state	Debugs ATM HA state information on the networking device.

debug atm ha-events

To debug ATM high-availability (HA) events on the networking device, use the **debug atm ha-events** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug atm ha-events

no debug atm ha-events

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.

Examples

The following example displays debug messages regarding ATM HA events on the networking device:

```
router# debug atm ha-events
```

Related Commands

Command	Description
debug atm ha-error	Debugs ATM HA errors on the networking device.
debug atm ha-state	Debugs ATM HA state information on the networking device.

debug atm ha-state

To debug ATM high-availability (HA) state information on the networking device, use the **debug atm ha-state** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug atm ha-state

no debug atm ha-state

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.

Examples

The following example displays debug messages regarding the ATM HA state on the networking device:

```
router# debug atm ha-state
```

Related Commands

Command	Description
debug atm ha-error	Debugs ATM HA errors on the networking device.
debug atm ha-events	Debugs ATM HA events on the networking device.

debug frame-relay redundancy

To debug Frame Relay redundancy on the networking device, use the **debug frame-relay redundancy** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug frame-relay redundancy

no debug frame-relay redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 7500 and 10000 series Internet routers.

Usage Guidelines

Use this command to debug Frame Relay synchronization problems. The **debug frame-relay redundancy** command logs synchronization events and errors.

Examples

The following example displays debug messages regarding Frame Relay redundancy on the networking device:

```
router# debug frame-relay redundancy
```

Related Commands

Command	Description
frame-relay redundancy auto-sync lmi-sequence-numbers	Configures LMI synchronization parameters.

debug ppp redundancy

To debug PPP synchronization on the networking device, use the **debug ppp redundancy** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug ppp redundancy [**detailed** | **event**]

no debug ppp redundancy [**detailed** | **event**]

Syntax Description

detailed	(Optional) Displays detailed debug messages related to specified PPP redundancy events.
event	(Optional) Displays information about protocol actions and transitions between action states (pending, waiting, idle) on the link.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 7500, 10000, and 12000 series Internet routers.

Examples

The following example displays detailed debug messages related to specified PPP redundancy events:

```
router# debug ppp redundancy detailed
```

debug redundancy

To enable the display of events for troubleshooting dual Route Processors (RPs), use the **debug redundancy** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug redundancy {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

no debug redundancy {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

Syntax Description

ehsa	Displays redundancy facility (RF) enhanced high system availability (EHSA) information.
errors	Displays RF errors.
fsm	Displays RF feasible successor metrics (FSM) events.
kpa	Displays RF keepalive events.
msg	Displays RF messaging events.
progression	Displays RF progression events.
status	Displays RF status events.
timer	Displays RF timer events.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(6)AA	This command was introduced.
12.0(15)ST	This command was introduced on Cisco 10000 series Internet routers.
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.

Examples

The following example enables debugging information for RF keepalive events:

```
router# debug redundancy kpa
```

frame-relay redundancy auto-sync lmi-sequence-numbers

To configure automatic synchronization of Frame Relay Local Management Interface (LMI) sequence numbers, use the **frame-relay redundancy auto-sync lmi-sequence-numbers** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

frame-relay redundancy auto-sync lmi-sequence-numbers

no frame-relay redundancy auto-sync lmi-sequence-numbers

Syntax Description

This command has no arguments or keywords.

Defaults

Automatic synchronization of Frame Relay LMI sequence numbers is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500 and 10000 series Internet routers.

Usage Guidelines

Enabling the **frame-relay redundancy auto-sync lmi-sequence-numbers** command improves the chances of a clean switchover on Frame Relay DTE interfaces when the peer Frame Relay DCE is intolerant of LMI errors. Use this command to configure LMI if the DCE fails the line protocol after fewer than three LMI errors and if changing the DCE configuration is neither possible nor practical.

Examples

The following example enables synchronization of LMI DTE sequence numbers on a router that is running Frame Relay:

```
frame-relay redundancy auto-sync lmi-sequence-numbers
```

Related Commands

Command	Description
debug frame-relay redundancy	Debugs Frame Relay redundancy on the networking device.

mode (redundancy)

To configure the redundancy mode of operation, use the **mode** command in redundancy configuration mode.

Cisco 7500 Series Internet Routers

mode {**hsa** | **rpr** | **rpr-plus** | **sso**}

Cisco 10000 Series Internet Routers

mode {**rpr-plus** | **sso**}

Cisco 12000 Series Internet Routers

mode {**rpr** | **rpr-plus** | **sso**}

Syntax Description

hsa	High system availability (HSA) redundancy mode.
rpr	Route Processor Redundancy (RPR) redundancy mode.
rpr-plus	Route Processor Redundancy Plus (RPR+) redundancy mode.
sso	Stateful switchover (SSO) redundancy mode.

Defaults

The default mode for the Cisco 7500 series Internet routers is HSA.

The default mode for the Cisco 10000 series Internet routers is SSO.

The default mode for the Cisco 12000 series Internet routers is RPR.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(22)S	SSO support was added.

Usage Guidelines

The mode selected by the **mode** command in redundancy configuration mode must be fully supported by the image that has been set into both the active and standby Route Processors (RPs). A high-availability image must be installed into the RPs before RPR can be configured. Use the **hw-module slot image** command to specify a high-availability image to run on the standby RP.

Examples

The following example configures RPR+ redundancy mode on a Cisco 12000 series or Cisco 1000 series Internet router:

```
mode rpr-plus
```

The following example sets the mode to HSA on a Cisco 7500 series Internet router:

```
mode hsa
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
redundancy	Enters redundancy mode.
redundancy force-switchover	Switches control of a router from the active to the standby RP.
show redundancy	Displays current or historical status and related information on a redundant DSC.

redundancy

To enter redundancy mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(9)SL	This command was introduced.
12.0(16)ST	This command was introduced on Cisco 7500 series Internet routers.
12.0(22)S	This command was introduced on Cisco 10000 series Internet routers.

Usage Guidelines

After you enter the **redundancy** command, the system prompt changes from `router#` to `router(config-red)#`, indicating that the router is in redundancy mode.

Examples

In the following example, the user enters redundancy mode from global configuration mode:

```
router(config)# redundancy
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active to the standby RP.
show redundancy	Displays current or historical status and related information on redundant DSC.

redundancy force-switchover

To switch control of a router from the active to the standby Route Processor (RP), use the **redundancy force-switchover** command in privileged EXEC mode.

redundancy force-switchover

Cisco 10000 Series Internet Routers

redundancy force-switchover main-cpu

Syntax Description

main-cpu	Forces switchover to the standby RP.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(16)ST	This command was introduced on Cisco 7500 series Internet routers.
12.0(17)ST	This command was introduced on Cisco 12000 series Internet routers.
12.0(22)S	This command replaces the **force-failover** command on Cisco 10000 series Internet routers.

Usage Guidelines

Use the **redundancy force-switchover** command to force a switchover between dual RPs, with the standby RP becoming the new active RP. Before switching over, the system verifies that the standby RP is ready to take over.

Examples

The following example forces a switchover to the standby RP on the Cisco 10000 series Internet routers:

```
router# redundancy force-switchover main-cpu
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy	Enters redundancy mode.
show redundancy	Displays current or historical status and related information on redundant DSC.

reload

To reload the operating system, use the **reload** command in EXEC mode.

Cisco 10000 and 7500 Series Internet Routers

reload [*line* | **at** *hh*:*mm* | **cancel** | **in** [*hh*:]*mm* [*line*]

Cisco 12000 Series Internet Routers

reload [*line* | **in** [*hh*:]*mm* [*line*] | **at** *hh*:*mm* [*month day* | *day month*] [*line*] | **cancel** | **slot** *slot-number* | **standby-cpu**]

Syntax Description

line	(Optional) Reason for the reload, 1 to 255 characters long.
in [*hh*:]*mm*	(Optional) Schedule a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. If you choose the *hh* argument, you must type the colon.
at *hh*:*mm*	(Optional) Schedule a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days. If you choose the *hh* argument, you must type the colon.
month	(Optional) Name of the month, any number of characters in a unique string.
day	(Optional) Number of the day in the range from 1 to 31.
cancel	(Optional) Cancel a scheduled reload.
slot	(Optional) A slot on a device.
slot-number	(Optional) The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
standby-cpu	(Optional) Reloads the standby route processor if present.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	The **standby-cpu** and **slot** keywords were added to the Cisco 12000 series Internet router platform.

Usage Guidelines

The **reload** command halts the system. If the system is set to restart on error, it reboots itself. Use the **reload** command after configuration information is entered into a file and saved to the startup configuration.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. Not setting up for automatic booting prevents the system from dropping to the ROM monitor and thereby taking the system out of the remote user control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system asks you if you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you enter "yes" in this situation, the system goes to setup mode upon reload.

When you schedule a reload to occur at a later time, it must take place within approximately 24 days.

The **at** keyword can be used only if the system clock has been set on the router (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, the time on each router must be synchronized with NTP.

To display information about a scheduled reload, use the **show reload** command.

Examples

The following example immediately reloads the software on the router:

```
Router# reload
```

The following example reloads the software on the router in 10 minutes:

```
Router# reload in 10
Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload? [confirm]
Router#
```

The following example reloads the software on the router at 1:00 p.m. today:

```
Router# reload at 13:00
Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Router#
```

The following example reloads the software on the router on April 20 at 2:00 a.m.:

```
Router# reload at 02:00 apr 20
Router# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Router#
```

The following example cancels a pending reload:

```
Router# reload cancel
%Reload cancelled.
```

show redundancy

To display current or historical status, mode, and related redundancy information about the device, use the **show redundancy** command in privileged EXEC mode.

show redundancy [**clients** | **counters** | **history** | **states** | **switchover history**]

Cisco 12000 Series Internet Routers

show redundancy [**all** | **arbitration** | **clients** | **counters** | **history** | **switchover history** | **mode-supported** | **standby** | **states** | **trace** | **trace all**]

Syntax Description

clients	(Optional) Displays the RF client list.
counters	(Optional) Displays the RF operational counters.
history	(Optional) Displays the RF history.
states	(Optional) Displays the RF states.
switchover history	(Optional) Displays switchover history information.
all	(Optional) Displays all of the redundancy mode output.
arbitration	(Optional) Displays details of the Redundancy Facility (RF) arbitration scheme.
mode-supported	(Optional) Displays a list of line cards supporting SSO.
standby	(Optional) Displays details of the current standby device.
trace	(Optional) Displays a trace of the main events for the redundancy finite state machine.
trace all	(Optional) Displays all basic and latest event traces.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced.
12.0(16)ST	This command was modified to show information on Route Processor Redundancy (RPR).
12.0(22)S	This command was modified to add the **switchover history** and **mode-supported** keyword combinations.

Usage Guidelines

Use this command to display the redundancy of Cisco IOS series Internet routers.

Examples

The following example shows redundancy client information for the Cisco 12000 series Internet router:

```
Router# show redundancy client

clientID = 0      clientSeq = 0        RF_INTERNAL_MSG
 clientID = 25     clientSeq = 130      CHKPT RF
 clientID = 27     clientSeq = 132      C12K RF COMMON Client
 clientID = 30     clientSeq = 135      Redundancy Mode RF
 clientID = 22     clientSeq = 140      Network RF Client
 clientID = 24     clientSeq = 150      CEF RRP RF Client
 clientID = 37     clientSeq = 151      MDFS RRP RF Client
 clientID = 5      clientSeq = 170      RFS client
 clientID = 23     clientSeq = 220      Frame Relay
 clientID = 49     clientSeq = 225      HDLC
 clientID = 20     clientSeq = 310      IPROUTING NSF RF cli
 clientID = 21     clientSeq = 320      PPP RF
 clientID = 34     clientSeq = 330      SNMP RF Client
 clientID = 29     clientSeq = 340      ATM
 clientID = 35     clientSeq = 350      History RF Client
 clientID = 50     clientSeq = 530      SNMP HA RF Client
 clientID = 65000  clientSeq = 65000    RF_LAST_CLIENT
```

The following example shows redundancy switchover history information:

```
router# show redundancy switchover history

Index   Prev Active     Curr Active     Swact Reason    Swact Time
1             1               0       unsupported     8:03:52 UTC Thu Nov 29 2001
2             0               1         unsupported      08:07:00 UTC Thu Nov 29 2001
```

Table 3 describes the significant fields shown in the display.

Table 3 Redundancy switchover history fields

Field	Description
Prev Active	Slot number of the previously active unit.
Curr Active	Slot number of the currently active unit.
Swact Reason	Reason for the switchover.
Swact Time	The date and time (*hours:minutes:seconds*) of the last switchover to the active RP.

The following example shows redundancy history information on a Cisco 12000 series Internet router:

```
router# show redundancy history

Redundancy Facility Event Log:
4w5d client added: RF_INTERNAL_MSG(0) seq=0
4w5d client added: RF_LAST_CLIENT(65000) seq=65000
4w5d client added: CHKPNT RF(25) seq=130
00:00:20 client added: C12K RF COMMON Client(27) seq=132
00:00:20 client added: RFS Client(5) seq=170
00:00:20 client added: History RF Client(35) seq=350
00:00:20 client added: Redundancy Mode RF(30) seq=135
```

The following example shows redundancy states information on a Cisco 10000 series Internet router:

```
router# show redundancy states

       my state = 13 -ACTIVE
```

```
    peer state = 8  -STANDBY HOT
          Mode = Duplex
          Unit = Preferred Primary
       Unit ID = 0

Maintenance Mode = Disabled
    Manual Swact = Enabled
  Communications = Up

           client count = 13
client_notification_TMR = 30000 milliseconds
         keep_alive TMR = 4000 milliseconds
       keep_alive count = 0
   keep_alive threshold = 7
          RF debug mask = 0x0
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy	Enters redundancy mode.
redundancy force-switchover	Switches control of a router from the active to the standby RP.