



# CHAPTER 24

## Configuring NSF with SSO MSFC Redundancy

---

This chapter describes how to configure MSFC redundancy using Cisco nonstop forwarding (NSF) with stateful switchover (SSO) on the Catalyst 6500 series switches.

**Note**

---

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series MSFC Cisco IOS Command Reference*.

---

**Note**

---

The term *MSFC* is used throughout this chapter to refer to MSFC2, MSFC2A, and MSFC3 except where specifically differentiated.

---

**Note**

---

Except where specifically differentiated, the information and procedures in this chapter apply to Supervisor Engine 32 with PFC3B/PFC3BXL, Supervisor Engine 720 with PFC3A/PFC3B/PFC3BXL, and Supervisor Engine 2 with PFC2.

---

This chapter consists of these sections:

- [Hardware and Software Requirements, page 24-2](#)
- [Understanding How NSF/SSO Works, page 24-2](#)
- [RPR Overview, page 24-3](#)
- [Types of MSFC Switchovers, page 24-4](#)
- [Configuration Guidelines and Restrictions, page 24-4](#)
- [Using the CLI to Configure NSF/SSO, page 24-5](#)
- [Upgrading Software, page 24-14](#)

# Hardware and Software Requirements

This section describes the hardware and software requirements for configuring NSF/SSO:

- Supported supervisor engines— Supervisor Engine 2, Supervisor Engine 720, and Supervisor Engine 32 (NSF/SSO is not supported with Supervisor Engine 1).
- Supported MSFCs—MSFC2, MSFC2A, and MSFC3 (the MSFC is not supported).
- The redundant supervisor engines must be the same type with the same model PFC and MSFC.
- Catalyst software release 8.5(1) and later releases.



## Note

If SSO is enabled on the MSFC, you must enable high availability on the supervisor engine *before* upgrading to supervisor engine software release 8.5(1) and later releases. Use the **set system highavailability enable** command to enable high availability on the supervisor engine.

- Cisco IOS Release 12.2(18)SXF and later releases.

# Understanding How NSF/SSO Works



## Note

SSO replaces single router mode (SRM) and dual router mode (DRM). There is no support for these high-availability modes. For SRM and DRM CLI processing details, see the [“Configuration Guidelines and Restrictions” section on page 24-4](#).

The Catalyst operating system that runs on the supervisor engine provides a Layer 2 high availability for redundant supervisor engines. Cisco IOS Release 12.2(18)SXF and later releases with NSF and SSO that run on the MSFC provide Layer 3 (and above) high availability for redundant MSFCs. MSFC SSO high-availability benefits are as follows:

- Reduced downtime.
- The ability to upgrade software without shutting down the MSFC.
- The ability to detect a failure of the active MSFC and allow the standby MSFC to take over the system with minimal drops in existing traffic flows.

When the system comes up, after the supervisor engine completes its initialization and prepares itself for operation, the supervisor engine sends an SCP inventory message to both MSFCs. The inventory message contains information about which MSFCs are present in the system and as other operational state information. From a high-availability perspective, the inventory message is important because it contains information that dictates which MSFC will be the active MSFC and which will be the standby MSFC.

During the startup of the standby MSFC, image version information is exchanged between MSFCs and one of the following occurs:

- If the image version information matches and both MSFCs are configured as SSO or have the default (SSO) configuration, the system runs in SSO mode.
- If the image version information does not match or if one of the MSFCs is configured for route processor redundancy (RPR), the system runs in RPR mode.

In NSF/SSO mode, one MSFC is active and the other MSFC is in a hot-standby mode. The hot-standby MSFC maintains a constant readiness state by receiving state information from the active MSFC. At any given moment, the standby MSFC may be called on by the supervisor engine to take over the responsibilities held by the active MSFC. The supervisor engine monitors the active MSFC and if the MSFC does not respond, the supervisor engine declares the MSFC as lost or down and proceeds to reset the MSFC. The standby MSFC has the up-to-date state information necessary to resume processing (the standby MSFC is fully initialized, but the VLANs are kept in an administrative down state until a switchover occurs).

With NSF, the switching modules and switch fabric continue to forward packets while the MSFC switchover is in progress.

**Note**

---

Detected failures of hardware or CLI commands may also cause a switchover.

---

**Note**

---

High availability on the supervisor engine operates independent of the MSFC high-availability feature. However, you must enable high availability on the supervisor engine must be enabled to ensure the correct operation of the MSFC SSO feature.

---

If you run the MSFC in SSO mode and fail to run the high-availability feature on the supervisor engine, any switchover that may occur will result in a nonstateful switchover and the standby MSFC will reset itself and reload at the time of the switchover. This reset/reload of the standby MSFC occurs because there is insufficient state information on the supervisor engine to support a stateful switchover of the MSFC. This reset/reload of the standby MSFC interrupts service.

---

## RPR Overview

**Note**

---

RPR+ mode is not supported.

---

RPR is a *cold* standby mode. When a switchover occurs, the standby MSFC must go completely through its initialization. RPR mode is used primarily for the fast software upgrade (FSU). (See the “[Fast Software Upgrade](#)” section on page 24-14.) In RPR mode, the startup configuration is synchronized to the standby MSFC, however, it is not processed in any way until the switchover occurs. The running configuration is not synchronized to the standby MSFC.

When the active MSFC boots completely, no state information is exchanged between the MSFCs. If the active MSFC fails, the standby MSFC processes its startup configuration file and begins its initialization.

If there is an image compatibility problem, the active MSFC boots fully, but the standby MSFC suspends its startup before processing the startup configuration file. If the active MSFC fails, a switchover is triggered and the suspended standby MSFC begins to initialize and become the active MSFC.

**Note**

---

High availability on the supervisor engine does not have to be enabled to run RPR on the MSFC.

---

## Types of MSFC Switchovers

The types of MSFC switchovers are as follows:

- Failover—An MSFC failover occurs when the active MSFC crashes or detects a serious system failure and ends up in ROMMON.
- Forced switchover—A forced switchover is caused by either entering a CLI command or by removing the supervisor engine with the active MSFC from the chassis. The MSFC CLI commands that force a switchover are the **redundancy force-switchover** and **reload** commands. The supervisor engine CLI command that forces a switchover is the **reset mod** command where *mod* is the module number of the MSFC as shown in the **show module** command display.

## Configuration Guidelines and Restrictions

This section describes the configuration guidelines and restrictions for configuring NSF/SSO:

- If SSO is enabled on the MSFC, you must enable high availability on the supervisor engine *before* upgrading to supervisor engine software release 8.5(1) and later releases. Use the **set system highavailability enable** command to enable high availability on the supervisor engine.
- SSO replaces SRM and DRM. There is no support for these high-availability modes. The details are as follows:
  - SRM CLI processing—Cisco IOS Release 12.2(18)SXF and later software releases contain the SRM CLI. The CLI is accepted when entered but it is not acted on in any way. The SRM CLI was kept in Cisco IOS Release 12.2(18)SXF and later software releases to assist you in migrating to NSF/SSO. However, the SRM CLI does not cause NVRAM updates. If you have SRM CLI in your configuration and you decide to modify the SRM configuration and enter the **write mem** command, the SRM CLI commands in the configuration are lost. If you want to downgrade to an image that has SRM, your original SRM CLI configuration is lost and you will have to reconfigure SRM. For this reason, we recommend that you save your configuration before you upgrade from SRM to NSF/SSO.
  - DRM CLI processing—Unlike SRM CLI, any existing DRM CLI in the configuration file after upgrading to NSF/SSO are flagged as errors at system startup. You must reconfigure the switch and remove the DRM configuration. We recommend that you save your configuration before you upgrade from DRM to NSF/SSO.
- During a switchover, there will be traffic loss for traffic that is routed by the MSFC. NSF only applies to traffic that is hardware switched by modules and the switch fabric. New flows are not allowed until the switchover is complete.
- In cases where the MSFC has failed and is unable to notify the supervisor engine of the failure, the supervisor engine may take 30 to 40 seconds before it realizes that the MSFC has failed and a switchover is triggered. If the supervisor engine receives the failure notification, the switchover is triggered immediately.
- The Frame Relay, ATM, and PPP protocols that are not supported in SSO mode.
- WAN modules react to SSO switchovers as follows:
  - WAN modules do not reload with an SSO switchover.
  - WAN module interfaces go down and then come back up during an SSO switchover.
  - All routing protocols do not perform NSF if NSF is configured over WAN interfaces.
  - All features on the WAN interfaces resume operation after an SSO switchover.

- Standby supervisor engine/MSFC insertion—With NSF/SSO redundancy, you can hot swap the standby supervisor engine/MSFC for maintenance. When you hot insert the standby MSFC, the active MSFC detects the presence of the standby MSFC and starts to drive the standby MSFC state transition to hot-standby. When you remove the standby MSFC, the synchronization between the active and standby MSFC is stopped, any pending updates to the standby MSFC are discarded, and the system enters simplex mode. The standby MSFC state is displayed by entering the **show redundancy states** command.
- Counters and statistics—The various counters and statistics that are maintained by the MSFC are not synchronized between MSFCs.
- Not all subsystems are high-availability aware and those that are high-availability aware may have their own set of limitations.
- Some subsystems have their own high availability-specific configurations and status commands (such as the **show isis nsf** command).
- MSFC software images do not currently support the in-service software upgrade (ISSU).
- Diagnostics are not integrated into high availability. Switchovers due to failed diagnostics on the MSFC are not supported.

## Using the CLI to Configure NSF/SSO

These sections describe how to configure NSF/SSO:

- [Configuring SSO, page 24-6](#)
- [Configuring CEF NSF, page 24-7](#)
- [Verifying CEF NSF, page 24-7](#)
- [Configuring BGP NSF, page 24-8](#)
- [Verifying BGP NSF, page 24-8](#)
- [Configuring OSPF NSF, page 24-9](#)
- [Verifying OSPF NSF, page 24-10](#)
- [Configuring IS-IS NSF, page 24-10](#)
- [Verifying IS-IS NSF, page 24-11](#)
- [Displaying Redundancy-Related Information, page 24-13](#)
- [Performing an MSFC Switchover, page 24-13](#)
- [Performing an MSFC Software Reload, page 24-13](#)
- [Using Redundancy-Related Debug Commands, page 24-13](#)

## Configuring SSO

SSO is the default mode. By default, even if you do not configure the system explicitly as SSO, the system comes up in SSO mode. However, we recommend that you explicitly configure SSO mode.



**Note** The following task can also be used to configure RPR mode (use **mode rpr** instead of **mode sso**).

To configure SSO mode, perform this task:

	Task	Command
<b>Step 1</b>	Enter redundancy configuration mode.	Router(config)# <b>redundancy</b>
<b>Step 2</b>	Configure SSO. When this command is entered, the redundant MSFC is reloaded and begins to work in SSO mode.	Router(config-red)# <b>mode sso</b>
<b>Step 3</b>	Verify that SSO is enabled.	Router# <b>show running-config</b>
<b>Step 4</b>	Display the operating redundancy mode.	Router# <b>show redundancy states</b>

This example shows how to configure the system for SSO and display the redundancy state:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# end
Router# show redundancy states
my state = 13 -ACTIVE
  peer state = 1 -DISABLED
    Mode = Simplex
    Unit = Primary
    Unit ID = 7
Redundancy Mode (Operational) = Stateful SwitchOver - SSO
Redundancy Mode (Configured) = Stateful SwitchOver - SSO
Redundancy State = Non Redundant

  Split Mode = Disabled
  Manual Swact = Disabled Reason: Simplex mode
  Communications = Down Reason: Simplex mode

  client count = 18
  client_notification_TMR = 30000 milliseconds
  keep_alive TMR = 9000 milliseconds
  keep_alive count = 0
  keep_alive threshold = 18
  RF debug mask = 0x0
Router#
```

## Configuring CEF NSF

CEF NSF operates by default while the networking device is running in SSO mode. No configuration is necessary.

## Verifying CEF NSF

To verify that CEF is NSF-capable, perform this task:

Task	Command
Verify that CEF is NSF-capable.	Router# <b>show cef state</b>

This example shows how to verify that CEF is NSF-capable:

```

router# show cef state
CEF Status [RP]
  CEF enabled/running
  dCEF enabled/running
  CEF switching enabled/running
  CEF default capabilities:
    Always CEF switching:          yes
    Always dCEF switching:         yes
    Default CEF switching:         yes
    Default dCEF switching:        yes
    Drop multicast packets:        no
    OK to punt packets:            yes
    NVGEN CEF state:               yes
    fastsend() used:               no
    CEF NSF capable:               yes
    RPR+/SSO standby capable:      yes
    IPC delayed func on SSO:       no
    FIB auto repair supported:      yes
    LCs not running at init time:   yes
    Hardware forwarding supported:  yes
    Hardware forwarding in use:     yes
    Load-sharing pr. packet supported: no
  RRP state:
    I am standby RRP:              no
    RF Peer Presence:               no
    RF PeerComm reached:           no
    Config Redundancy mode:         Stateful SwitchOver - SSO(7)
    Operating Redundancy mode:      Stateful SwitchOver - SSO(7)
    CEF NSF:                         enabled/not running
  RP state:
    Expanded LC ipc memory:         0 Kbytes
    Linecard reloader type:         aggressive (Default)
    Linecard dFIB structures:       initialized
Router#

```

## Configuring BGP NSF



**Note** You must configure BGP graceful restart on all peer devices that participate in BGP NSF.

To configure BGP for NSF, perform this task (repeat this procedure on each of the BGP NSF peer devices):

	Purpose	Command
<b>Step 1</b>	Enter global configuration mode.	Router# <b>configure terminal</b>
<b>Step 2</b>	Enable a BGP routing process, which places the router in router configuration mode.	Router(config)# <b>router bgp</b> <i>as-number</i>
<b>Step 3</b>	Enable the BGP graceful restart capability, starting BGP NSF.  If you enter this command after the BGP session has been established, you must restart the session for the capability to be exchanged with the BGP neighbor.  Use this command on the restarting router and all of its peers.	Router(config-router)# <b>bgp graceful-restart</b>

## Verifying BGP NSF

To verify BGP NSF, you must check that the graceful restart function is configured on the SSO-enabled networking device and on the neighbor devices. To verify, follow these steps:

**Step 1** Verify that “bgp graceful-restart” appears in the BGP configuration of the SSO-enabled router by entering the **show running-config** command:

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

**Step 2** Repeat step 1 on each of the BGP neighbors.

- Step 3** On the SSO device and the neighbor device, verify that the graceful restart function is shown as both advertised and received, and confirm the address families that have the graceful restart capability.



**Note** If no address families are listed, then BGP NSF also will not occur.

```
Router# show ip bgp neighbors x.x.x.x

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

## Configuring OSPF NSF



**Note** All peer devices that participate in OSPF NSF must be made OSPF NSF-aware, which happens automatically once you install an NSF software image on the device.

To configure OSPF NSF, perform this task:

	Purpose	Command
<b>Step 1</b>	Enter global configuration mode.	Router# <b>configure terminal</b>
<b>Step 2</b>	Enable an OSPF routing process, which places the router in router configuration mode.	Router(config)# <b>router ospf processID</b>
<b>Step 3</b>	Enable NSF operations for OSPF.	Router(config-router)# <b>nsf</b>

## Verifying OSPF NSF

To verify OSPF NSF, you must check that the NSF function is configured on the SSO-enabled networking device. To verify OSPF NSF, follow these steps:

- Step 1** Verify that “nsf” appears in the OSPF configuration of the SSO-enabled device by entering the **show running-config** command.

```
Router# show running-config

router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
.
.
.
```

- Step 2** Verify that NSF is enabled on the device by entering the **show ip ospf** command.

```
router> show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
Area has no authentication
SPF algorithm executed 3 times
```

## Configuring IS-IS NSF

To configure IS-IS NSF, perform this task:

	Purpose	Command
<b>Step 1</b>	Enter global configuration mode.	Router# <b>configure terminal</b>
<b>Step 2</b>	Enable an IS-IS routing process, which places the router in router configuration mode.	Router(config)# <b>router isis</b> [tag]

	Purpose	Command
Step 3	<p>Enable NSF operation for IS-IS.</p> <p>Enter the <b>ietf</b> keyword to enable IS-IS in a homogeneous network where adjacencies with networking devices supporting IETF draft-based restartability is guaranteed.</p> <p>Enter the <b>cisco</b> keyword to run IS-IS in heterogeneous networks that might not have adjacencies with NSF-aware networking devices.</p>	Router(config-router)# <b>nsf</b> [ <b>cisco</b>   <b>ietf</b> ]
Step 4	(Optional) Specify the minimum time between NSF restart attempts. The default time between <i>consecutive</i> NSF restart attempts is 5 minutes.	Router(config-router)# <b>nsf interval</b> [ <i>minutes</i> ]
Step 5	<p>(Optional) Specify the time that IS-IS will wait for the IS-IS database to synchronize before generating overloaded link-state information for itself and flooding that information out to its neighbors.</p> <p>The <b>t3</b> keyword applies only if you selected IETF operation. When you specify <b>adjacency</b>, the router that is restarting obtains its wait time from neighboring devices.</p>	Router(config-router)# <b>nsf t3</b> { <b>manual</b> [ <i>seconds</i> ]   <b>adjacency</b> }
Step 6	(Optional) Specify how long an IS-IS NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart. The default is 10 seconds.	Router(config-router)# <b>nsf interface wait</b> <i>seconds</i>

## Verifying IS-IS NSF

To verify IS-IS NSF, you must check that the NSF function is configured on the SSO-enabled networking device. To verify IS-IS NSF, perform these steps:

- Step 1** Verify that “nsf” appears in the IS-IS configuration of the SSO-enabled device by entering the **show running-config** command. The display will show either the Cisco IS-IS or the IETF IS-IS configuration. This example indicates that the device uses the Cisco implementation of IS-IS NSF:

```
Router# show running-config
<...Output Truncated...>
router isis
nsf cisco
<...Output Truncated...>
```

- Step 2** If the NSF configuration is set to **cisco**, enter the **show isis nsf** command to verify that NSF is enabled on the device. Using the Cisco configuration, the display output will be different on the active and redundant MSFCs (RPs). This example shows the sample output for the Cisco configuration on the active MSFC (RP). In this example, note the presence of “NSF restart enabled”:

```
router# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
```

```
Local state:ACTIVE, Peer state:STANDBY HOT, Mode:SSO
```

This example shows the sample output for the Cisco configuration on the standby RP. In this example, note the presence of “NSF restart enabled”:

```
router# show isis nsf

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

**Step 3** If the NSF configuration is set to **ietf**, enter the **show isis nsf** command to verify that NSF is enabled on the device. This example shows the sample output for the IETF IS-IS configuration on the networking device:

```
router# show isis nsf

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

## Displaying Redundancy-Related Information

Use the **show redundancy** [qualifier] command to display redundancy-related information. The supported qualifiers are as follows:

```
Router# show redundancy ?
  clients          Redundancy Facility (RF) client list
  counters         Redundancy Facility (RF) operational counters
  events           Redundancy Facility (RF) events list
  history          Redundancy Facility (RF) history
  linecard-group   Line card redundancy group information
  states           Redundancy Facility (RF) states
  switchover       Redundancy Facility (RF) switchover
  |               Output modifiers
  <cr>

Router#
```

## Performing an MSFC Switchover

Use the **redundancy switch-activity** [force] command to switch over to the standby MSFC. The **force** keyword overrides any restrictions.

## Performing an MSFC Software Reload

Use the **redundancy reload** {peer | shelf} command to reload the standby MSFC (**peer** keyword) or all modules in the chassis (**shelf** keyword).

## Using Redundancy-Related Debug Commands

Use the **debug redundancy** [qualifier] command to display redundancy-related debug information. The supported qualifiers are as follows:

```
Router# debug redundancy ?
  config-sync     HA config sync debug option
  ehsa            Redundancy Facility (RF) EHSA
  errors          Redundancy Facility (RF) Errors
  fsm            Redundancy Facility (RF) FSM events
  kpa            Redundancy Facility (RF) keep alive
  msg            Redundancy Facility (RF) Messaging events
  progression     Redundancy Facility (RF) Progression events
  status         Redundancy Facility (RF) Status events
  timer          Redundancy Facility (RF) Timer events

Router#
```

Use the **debug hybrid-ha** [qualifier] command to display NSF/SSO-specific redundancy information. The supported qualifiers are as follows:

```
Router# debug hybrid-ha ?
  all            All Hybrid HA SSO/NSF platform specific debugging messages
  errors        Hybrid HA SSO/NSF platform specific warnings and errors
  events       Hybrid HA SSO/NSF platform specific events
  ipc         Hybrid HA SSO/NSF platform specific IPC related events
  kpa        Hybrid HA SSO/NSF platform specific Keep-Alive related events

Router#
```

# Upgrading Software

These sections describe how to upgrade the MSFC software:

- [Fast Software Upgrade, page 24-14](#)
- [Upgrading to SSO from Single Router or Dual Router Modes, page 24-15](#)
- [Mixed-Mode Operation, page 24-15](#)



**Note**

Before performing any software upgrade procedure, see the [“Configuration Guidelines and Restrictions” section on page 24-4](#).

## Fast Software Upgrade



**Note**

Because the system is in RPR mode during the fast software upgrade, service is interrupted. The switchover is not stateful; interfaces go down but come back up as the MSFC initializes and comes up in RPR mode. Additionally, any configuration changes that are not saved are lost.



**Note**

This procedure requires that the Cisco IOS Release on both MSFCs supports RPR (at a minimum), and both MSFCs must be running the same software version. The active MSFC checks the standby image version when the standby MSFC is coming up, and if the standby image version does not match the active image version, the redundancy mode falls back to RPR.



**Note**

This procedure does not work with SRM and DRM images.



**Note**

The redundant supervisor engines must be the same type with the same model PFC and MSFC.

The fast software upgrade allows you to reduce planned downtime for software upgrades or downgrades. The fast software upgrade procedure consists of loading a new image onto both the standby MSFC and the active MSFC, and then rebooting the standby MSFC. The new image running on the standby MSFC is incompatible with the image currently running on the active MSFC, so the standby MSFC comes up in RPR mode. The fast software upgrade is done in RPR mode to avoid image incompatibility during the upgrade process.

To bring the new images into service, the standby MSFC is forced to switch over by taking the active MSFC out of service; the standby MSFC now becomes the active MSFC. Next, the out-of-service MSFC is allowed to boot; it becomes the standby MSFC but runs the newly upgraded image. The new image is running on both MSFCs, and the standby MSFC comes up in the hot-standby state. At this point, the system is now running in SSO mode because both MSFCs are running the same image version.



**Note**

You may restore the original roles of the MSFCs (their active and passive status) by forcing another switchover in which the standby MSFC becomes the active MSFC.

To perform fast software upgrade procedure, perform these steps:

- 
- Step 1** Copy the new image to both MSFCs.
- Step 2** Set the boot variables and save the configuration by entering the **write memory** command.
- Step 3** Reset the standby MSFC and bring it back online, running the new image. Ensure the standby MSFC is fully online by entering the **show redundancy states** command.
- Step 4** Do a manual switchover by entering the **redundancy force-switchover** command. The standby MSFC becomes the newly active MSFC running the new image. Because the system was in RPR mode before the switchover, the installed modules are reset and redownloaded with the new software during the switchover.
- Step 5** After the new standby MSFC reboots and comes back online, both MSFCs and installed modules are running the new version of the software.
- 

## Upgrading to SSO from Single Router or Dual Router Modes



**Note** This upgrade interrupts service. The actual downtime varies based on the configuration of the switch, but it will not be longer than the time it takes to boot the system and come online.



**Note** When upgrading to SSO from SRM or DRM, you must save your configuration before performing the upgrade. DRM configurations generate parse errors when the system reloads the new image. After the upgrade, DRM configurations need to be reconfigured for use with SSO.

Cisco IOS software prior to Cisco IOS Release 12.2(18)SXF is either SRM and/or DRM capable but does not support upgrading to SSO. These software images cannot be upgraded using the fast software upgrade procedure. To upgrade this software, you are required to load the new images on each of the MSFCs, and then simultaneously boot both MSFCs.

After the new images have been loaded on the MSFCs, you must reboot the system to load the new images. During this boot time, the switch is offline and you will not see the benefits of SSO until the new images are loaded.

## Mixed-Mode Operation

If you make a mistake when upgrading the software, it may result in a mixed-mode situation in which an SSO-based image is running on one MSFC and an SRM and/or DRM based image is running on the other MSFC. This situation could lead to system stability problems.

In this mixed mode, if the SSO-based image is running on the active MSFC, the active MSFC will boot completely, coming up in a simplex (nonredundant) state. The SRM and/or DRM based image will also boot but will remain in a standby state.

Another example of a mixed-mode upgrade scenario is when the SRM and/or DRM image is running on the active MSFC and the SSO-based image is running on the standby MSFC. In this mode, the active MSFC running the SRM and/or DRM image will boot completely, but the SSO-based image running on the standby MSFC will incorrectly determine that it is the active MSFC and will try to boot as the active MSFC. When the inventory message is received from the supervisor engine indicating it should be the standby MSFC, it will report an MSFC role mismatch error and reload itself. This problem can happen whenever an SRM, DRM, or boothelper image is running on the active MSFC and you try to load an SSO capable image on the standby MSFC.

To correct both scenarios, you must either upgrade the SRM and/or DRM software to the same level as the SSO-based software, or downgrade the SSO-based software to the level of the SRM and/or DRM image.