mail-server through service image-version efsu

mail-server

To configure an SMTP e-mail server address for Call Home, use the **mail-server**command in call home configuration mode. To remove one or all mail servers, use the **no** form of this command.

mail-server {*ipv4-addressname*} **priority** *number*
no mail-server {[{*ipv4-address* | *name* [**priority** *number*]}] | **all**}

Syntax Description

ipv4-address	IPv4 address of the mail server.
name	Fully qualified domain name (FQDN) of 64 characters or less.
priority *number*	Number from 1 to 100, where a lower number defines a higher priority.
all	Removes all configured mail servers.

Command Default

No e-mail server is configured.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE 16.11.a Gibraltar	The **no mail-server all** command is changed to **no mail-server**

Usage Guidelines

To support the e-mail transport method in the Call Home feature, you must configure at least one Simple Mail Transfer Protocol (SMTP) mail server using the **mail-server** command.

You can specify up to four backup e-mail servers, for a maximum of five total mail-server definitions.

Consider the following guidelines when configuring the mail server:

- Only IPv4 addressing is supported.
- Backup e-mail servers can be defined by repeating the mail-server command using different priority numbers.
- The mail-server priority number can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

Note Starting from Cisco IOS XE 16.11.a Gibraltar release, the configuration of **mail-server** command is case sensitive.

Examples

The following example configures two mail servers, where the mail server at "smtp.example.com" serves as the primary (with lower priority number than the second mail server), while the mail server at 192.168.0.1 serves as a backup:

```
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.168.0.1 priority 2
```

The following example shows how to remove configuration of both configured mail servers:

```
Router(cfg-call-home)# no mail-server all
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
show call-home	Displays Call Home configuration information.

mdr download reserve memory image

To reserve memory for preloading new software onto line cards that support enhanced Fast Software Upgrade (eFSU), use the **mdr download reserve memory image** command in privileged EXEC mode. To keep the router from reserving memory on line cards, use the **no** form of the command.

mdr download reserve memory image {**all-slots** | **slot** *slot-num*}
no mdr download reserve memory image {**all-slots** | **slot** *slot-num*}

Syntax Description

all-slots	Reserves memory for the new software on all installed line cards that support eFSU.
slot *slot-num*	Reserves memory for the new software on the line card in the specified chassis slot.

Command Default

This command is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on Cisco 7600 series routers.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

On line cards that support eFSU, the router automatically reserves memory on the line card to store the new software image (decompressed format). During the upgrade, the router preloads new line card software onto supported line cards. The amount of memory needed varies according to line card type.

You can issue the **show mdr download image**command to display the amount of memory that will be reserved on the line cards that support eFSU.

Although we do not recommend it, you can issue the **no mdr download reserve memory image** command to keep the router from reserving memory for software preload on the specified line card.

Note If a line card does not have enough memory available to hold the new software image, eFSU software preload fails and the line card undergoes a reset during software upgrade.

Examples

The following command reserves memory for the new software on the line card installed in slot 6:

```
Router# mdr download reserve memory image slot 6
```

Related Commands

Command	Description
show mdr download image	Displays the amount of memory that will be reserved for software preload on line cards that support eFSU.

mls ip multicast sso

To configure the stateful switchover (SSO) parameters, use the **mls ip multicast sso** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls ip multicast sso {**convergence-time** *time* | **leak** {**interval** *seconds* | **percent** *percentage*}}
no mls ip multicast sso {**convergence-time** *time* | **leak** {**interval** *seconds* | **percent** *percentage*}}

Syntax Description

convergence-time *time*	Specifies the maximum time to wait for protocol convergence; valid values are from 0 to 3600 seconds.
leak interval *seconds*	Specifies the packet-leak interval; valid values are from 0 to 3600 seconds.
leak percent *percentage*	Specifies the percentage of multicast packets leaked to the router during switchover so that protocol convergence can take place; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **convergence-time** *time* --20 seconds
- **leak** *interval* --60 seconds
- **leak** *percentage* --10 percent

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to set the maximum time to wait for protocol convergence to 300 seconds:

```
Router(config)#
mls ip multicast sso convergence-time 300
Router(config)#
```

This example shows how to set the packet-leak interval to 200 seconds:

```
Router(config)#
mls ip multicast sso leak interval 200
Router(config)#
```

This example shows how to set the packet-leak percentage to 55 percent:

```
Router(config)#
```

```
mls ip multicast sso leak percent 55
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast sso	Displays information about multicast high-availability SSO.

mode (redundancy)

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

Cisco 7304 Router
mode {**rpr** | **rpr-plus** | **sso**}

Cisco 7500 Series Routers
mode {**hsa** | **rpr** | **rpr-plus** | **sso**}

Cisco 10000 Series Routers
mode {**rpr-plus** | **sso**}

Cisco 12000 Series Routers
mode {**rpr** | **rpr-plus** | **sso**}

Cisco uBR10012 Universal Broadband Router
mode {**rpr-plus** | **sso**}

Syntax Description

rpr	Route Processor Redundancy (RPR) redundancy mode.
rpr-plus	Route Processor Redundancy Plus (RPR+) redundancy mode.
sso	Stateful Switchover (SSO) redundancy mode.
hsa	High System Availability (HSA) redundancy mode.

Command Default

The default mode for the Cisco 7500 series routers is HSA. The default mode for the Cisco 7304 router and Cisco 10000 series routers is SSO. The default mode for the Cisco 12000 series routers is RPR. The default mode for the Cisco uBR10012 universal broadband router is SSO.

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(22)S	SSO support was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support was added for the Cisco 7304 router. The Cisco 7500 series router is not supported in Cisco IOS Release 12.2(20)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Release	Modification
12.2(33)SCE	This command was modified in Cisco IOS Release 12.2(33)SCE. The rpr-plus keyword was removed.

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.

For Cisco IOS Release 12.2(33)SCA on the Cisco 10000 series routers and the Cisco uBR10012 universal broadband router, the use of SSO redundancy mode is recommended because RPR+ redundancy mode is being removed. If you enable RPR+ redundancy mode, you may see the following message:

```
*******************************************************
* Warning, The redundancy mode RPR+ is being deprecated *
* and will be removed in future releases. Please change *
* mode to SSO:                                          *
*     redundancy                                        *
*        mode sso                                       *
*******************************************************
```

Examples

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

```
Router# mode rpr-plus
```

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

```
Router# mode hsa
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby Route Processor (RP).
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces the standby Route Processor (RP) to assume the role of the active RP.
show redundancy	Displays current active and standby Performance Routing Engine (PRE) redundancy status.

monitor event-trace sbc (EXEC)

To monitor and control the event trace function for the Session Border Controller (SBC), use the **monitor event-trace sbc**command in privileged EXEC mode.

monitor event-trace sbc ha {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}

Syntax Description

ha	Monitors and controls event trace messages for SBC High Availability (HA).
clear	Clears existing trace messages for the SBC.
continuous	Continuously displays the latest event trace entries.
cancel	(Optional) Cancels the continuous display of latest trace entries.
disable	Turns off event tracing for the SBC.
dump	Writes the event trace results to the file configured using the **monitor event-trace sbc ha**command in global configuration mode. The trace messages are saved in binary format.
pretty	(Optional) Saves the event trace messages in ASCII format.
enable	Turns on event tracing for the SBC.
one-shot	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the **monitor event-trace sbc ha**command in global configuration mode.

Command Default

Event tracing for SBC is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.3	The **sbc_ha**keyword was changed to two keywords, **sbc** and **ha**.
Cisco IOS XE Release 2.4	The event tracing default for the **monitor event-trace sbc ha**commandwas changed from enabled to disabled.

Usage Guidelines

Use the **monitor event-trace sbc ha**command to control what, when, and how event trace data for the SBC on the Cisco ASR 1000 Series Aggregation Services Routers is collected.

Use this command after you have configured the event trace functionality on the Cisco ASR 1000 Series Routers using the **monitor event-trace sbc ha**command in global configuration mode.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace sbc ha**command in global configuration mode for each instance of a trace.

You can enable or disable SBC event tracing in one of two ways: using the **monitor event-trace sbc ha**command in privileged EXEC mode or using the **monitor event-trace sbc**command in global configuration mode. To disable event tracing, you would enter either of these commands with the disable keyword. To enable event tracing again, you would enter either of these commands with the enable keyword.

Use the **show monitor event-trace sbc ha**command to display trace messages. Use the **monitor event-trace sbc ha dump** command to save trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace sbc ha dump pretty** command.

To configure the file in which you want to save trace information, use the **monitor event-trace sbc ha dump-file***dump-file-name*command in global configuration mode. The trace messages are saved in binary format.

Examples

The following example shows the privileged EXEC commands that stop event tracing, clear the current contents of memory, and reenable the trace function for SBC HA events. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace sbc ha disable
Router# monitor event-trace sbc ha clear
Router# monitor event-trace sbc ha enable
```

The following example shows how to configure the continuous display of the latest SBC HA trace entries:

```
Router# monitor event-trace sbc ha continuous
```

The following example shows how to stop the continuous display of the latest trace entries:

```
Router# monitor event-trace sbc ha continuous cancel
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls the event trace function for a specified Cisco IOS software subsystem component.
monitor event-trace sbc (global)	Configures event tracing for the SBC.
show monitor event-trace	Displays event trace messages for Cisco IOS software subsystem components.

monitor event-trace sbc (global)

To configure event tracing for the Session Border Controller (SBC), use the **monitor event-trace sbc**command in global configuration mode. To remove an event tracing configuration for SBC, use the **no** form of this command.

monitor event-trace sbc ha {**disable** | **dump-file** *dump-file-name* | **enable** | **size** *number* | **stacktrace** [*depth*]}
no monitor event-trace sbc ha {**dump-file** *dump-file-name* | **size** *number* | **stacktrace** [*depth*]}

Syntax Description

ha	Configures event tracing for SBC high availability (HA).
disable	Turns off event tracing for SBC HA.
dump-file *dump -file-name*	Specifies the file where event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable	Turns on event tracing for SBC HA events if it had been disabled with the **monitor event-trace sbc ha disable**command.
size *number*	Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from 1 to 1000000. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace sbc ha parameters** command. When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace	Enables the stack trace at tracepoints. **Note** You must clear the trace buffer with the **monitor event-trace sbc ha clear** privileged EXEC command before entering this command.
depth	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.

Command Default

Event tracing for the SBC is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.3	The **sbc_ha**keyword was changed to two keywords, **sbc** and **ha**.
Cisco IOS XE Release 2.4	The event tracing default for the **monitor event-trace sbc ha**commandwas changed from enabled to disabled.

Usage Guidelines

Use the **monitor event-trace sbc ha**command to enable or disable event tracing and to configure event trace parameters for SBC.

The Cisco IOS XE software allows SBC to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace sbc ha**command in privileged EXEC mode or using the **monitor event-trace sbc ha**command in global configuration mode.

Additionally, default settings do not appear in the configuration file. If SBC enables event tracing by default, the **monitor event-trace sbc ha enable** command does not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem creates a command entry in the configuration file.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace sbc ha size**command for each instance of a trace. Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace sbc ha parameters** command.

To determine whether event tracing is enabled by default for SBC, use the **show monitor event-trace sbc ha**command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer with the **monitor event-trace sbc ha clear** privileged EXEC command.

Examples

The following example shows how to enable event tracing for SBC subsystem component in Cisco IOS XE software and configure the size to 10,000 messages. The trace messages file is set to sbc-ha-dump in flash memory.

```
Router(config)# monitor event-trace sbc ha enable
Router(config)# monitor event-trace sbc ha dump-file bootflash:sbc-ha-dump
Router(config)# monitor event-trace sbc ha size 10000
```

Related Commands

Command	Description
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace sbc (EXEC)	Monitors and controls the event trace function for the SBC.
show monitor event-trace sbc	Displays event trace messages for the SBC.

neighbor ha-mode sso

To configure a Border Gateway Protocol (BGP) neighbor to support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **neighbor ha-mode sso** command in the appropriate command mode. To remove the configuration, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **ha-mode sso**
no neighbor {*ip-address* | *ipv6-address*} **ha-mode sso**

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.

Command Default

BGP NSR with SSO support is disabled.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Session-template configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE 3.6S	This command was modified. It is supported in router configuration mode.
15.2(2)S	This command was modified. It is supported in router configuration mode.
Cisco IOS XE 3.7S	This command was implemented on the Cisco ASR 903 router.

Usage Guidelines

The **neighbor ha-mode sso** command is used to configure a BGP neighbor to support BGP NSR with SSO. BGP NSR with SSO is disabled by default.

BGP NSR with SSO is supported in BGP peer, BGP peer group, and BGP session template configurations. To configure BGP NSR with SSO in BGP peer and BGP peer group configurations, use the **neighbor ha-mode sso** command in address family configuration mode for address family BGP peer sessions. To include support for Cisco BGP NSR with SSO in a peer session template, use the **ha-mode sso** command in session-template configuration mode.

Examples

The following example shows how to configure a BGP neighbor to support SSO:

```
Router(config-router-af)# neighbor 10.3.32.154 ha-mode sso
```

Related Commands

Command	Description
show ip bgp sso summary	Displays the state of NSR established sessions for the IPv4 address family or all address families.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip bgp vpnv4 all sso summary	Displays the number of BGP neighbors that support SSO.

nsf (EIGRP)

To enable Cisco nonstop forwarding (NSF) operations for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **nsf** command in router configuration or address family configuration mode. To disable EIGRP NSF and to remove the EIGRP NSF configuration from the running-configuration file, use the **no** form of this command.

nsf
no nsf

Syntax Description

This command has no arguments or keywords.

Command Default

EIGRP NSF is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was modified. Support for Address family configuration mode was added.
12.2(33)SRE	This command was modified. Support for Address family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was modified. Support for IPv6 and IPv6 VPN Routing and Forwarding (VRF) was added.
15.2(2)S	This command was modified. Support for IPv6 and IPv6 VRF was added.

Usage Guidelines

The **nsf** command is used to enable or disable EIGRP NSF support on an NSF-capable router. NSF is supported only on platforms that support High Availability.

Examples

The following example shows how to disable NSF:

```
Device# configure terminal
Device(config)# router eigrp 101
```

```
Device(config-router)# no nsf
Device(config-router)# end
```

The following example shows how to enable EIGRP IPv6 NSF:

```
Device# configure terminal
Device(config)# router eigrp virtual-name-1
Device(config-router)# address-family ipv6 autonomous-system 10
Device(config-router-af)# nsf
Device(config-router-af)# end
```

Related Commands

Command	Description
debug eigrp address-family ipv6 notifications	Displays information about EIGRP address family IPv6 event notifications.
debug eigrp nsf	Displays notifications and information about NSF events for an EIGRP routing process.
debug ip eigrp notifications	Displays information and notifications for an EIGRP routing process.
show ip protocols	Displays the parameters and the current state of the active routing protocol process.
show ipv6 protocols	Displays the parameters and the current state of the active IPv6 routing protocol process.
timers graceful-restart purge-time	Sets the graceful-restart purge-time timer to determine how long an NSF-aware router that is running EIGRP must hold routes for an inactive peer.
timers nsf converge	Sets the maximum time that the restarting router must wait for the end-of-table notification from an NSF-capable or NSF-aware peer.
timers nsf signal	Sets the maximum time for the initial restart period.

nsf (IS-IS)

To configure Cisco nonstop forwarding (NSF) operations for Intermediate System-to-Intermediate System (IS-IS), use the **nsf** command in router configuration IS-IS 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.

nsf [{**cisco** | **ietf**}]
no nsf [{**cisco** | **ietf**}]

Syntax Description

cisco	(Optional) Enables Cisco proprietary IS-IS NSF.
ietf	(Optional) Enables IETF IS-IS NSF.

Command Default

NSF is disabled by default.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support for the Cisco 7304 router was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The user must configure NSF operation only if a router is expected to perform NSF during restart. The optional **cisco** keyword enables the use of checkpointing to allow the standby route processor (RP) to restore protocol state when an NSF restart occurs.

Examples

The following example enables Cisco proprietary IS-IS NSF operation:

```
nsf cisco
```

The following example enables IETF IS-IS NSF operation:

```
nsf ietf
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.

Command	Description
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf interval	Specifies the minimum time between NSF restart attempts.
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
show clns neighbors	Displays both ES and IS neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf (OSPF)

Note Effective with Cisco IOS Release 12.0(32)S, the **nsf** (OSPF) command has been replaced by the **nsf cisco** command. See the **nsf cisco** command for more information.

To configure Cisco nonstop forwarding (NSF) operations for Open Shortest Path First (OSPF), use the **nsf** command in router configuration mode. To disable Cisco NSF for OSPF, use the **no** form of this command.

nsf [**enforce global**]
no nsf [**enforce global**]

Syntax Description

enforce global	(Optional) Cancels NSF restart when non-NSF-aware neighboring networking devices are detected.

Command Default

This command is disabled by default; therefore, NSF operations for OSPF is not configured.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.0(32)S	This command was replaced by the **nsf cisco** command.

Usage Guidelines

The user must configure NSF operation for OSPF only if a router is expected to perform NSF during restart. For users to have full NSF benefits, all OSPF neighbors of the specified router must be NSF-aware.

If neighbors that are not NSF-aware are detected on a network interface, NSF restart is aborted on the interface; however, NSF restart will continue on other interfaces. This functionality applies to the default NSF mode of operation when NSF is configured.

If the user configures the optional **enforce global**keywords, NSF restart will be canceled for the entire process when neighbors that are not NSF-aware are detected on any network interface during restart. NSF restart will also be canceled for the entire process if a neighbor adjacency reset is detected on any interface or if an OSPF interface goes down. To revert to the default NSF mode, enter the **no nsf enforce global** command.

Examples

The following example enters router configuration mode and cancels the NSF restart for the entire OSPF process if neighbors that are not NSF-aware are detected on any network interface during restart:

```
Router(config)# router ospf 1
Router(config-router)# nsf cisco enforce global
```

Related Commands

Command	Description
debug ip ospf nsf	Displays debugging messages related to OSPF NSF commands.
router ospf	Enables OSPF routing and places the router in router configuration mode.

nsf cisco

To enable Cisco nonstop forwarding (NSF) operations on a router that is running Open Shortest Path First (OSPF), use the **nsf cisco** command in router configuration mode. To return to the default, use the **no** form of this command.

nsf cisco [{**enforce global** | **helper** [**disable**]}]
no nsf cisco [{**enforce global** | **helper disable**}]

Syntax Description

enforce global	(Optional) Cancels NSF restart on all interfaces when neighboring networking devices that are not NSF-aware are detected on any interface during the restart process.
helper	(Optional) Configures Cisco NSF helper mode.
disable	(Optional) Disables helper mode.

Command Default

Cisco NSF restarting mode is disabled. Cisco NSF helper mode is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(32)S	This command was introduced. This command replaces the **nsf**(OSPF) command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

For Cisco IOS Release 12.0(32)S and later releases, this command replaces the **nsf** (OSPF) command.

This command enables Cisco NSF on an OSPF router. When NSF is enabled on a router, the router is NSF-capable and will operate in restarting mode.

If a router is expected to cooperate with a neighbor that is doing an NSF graceful restart only, the neighbor router must be running a Cisco software release that supports NSF but NSF need not be configured on the router. When a router is running a Cisco software release that supports NSF, the router is NSF-aware.

By default, neighboring NSF-aware routers will operate in NSF helper mode during a graceful restart. To disable Cisco NSF helper mode on an NSF-aware router, use this command with the **disable** keyword. To reenable helper mode after explicitly disabling helper mode on an NSF-aware router, use the **no nsf cisco helper disable** command.

If neighbors that are not NSF-aware are detected on a network interface during an NSF graceful restart, restart is aborted on that interface only and graceful restart will continue on other interfaces. To cancel restart for the entire OSPF process when neighbors that are not NSF-aware are detected during restart, configure this command with the **enforce global** keywords.

Note The NSF graceful restart will also be canceled for the entire process when a neighbor adjacency reset is detected on any interface or when an OSPF interface goes down.

Examples

The following example enables Cisco NSF restarting mode on a router and causes the NSF restart to be canceled for the entire OSPF process if neighbors that are not NSF-aware are detected on any network interface during the restart.

```
router ospf 24
 nsf cisco enforce global
```

Related Commands

Command	Description
nsf ietf	Enables IETF NSF.

nsf ietf

To configure Internet Engineering Task Force (IETF) nonstop forwarding (NSF) operations on a router that is running Open Shortest Path First (OSPF), use the **nsf ietf** command in router configuration mode. To return to the default, use the **no** form of this command.

nsf ietf [{**restart-interval** *seconds* | **helper** [{**disable** | **strict-lsa-checking**}]}]
no nsf ietf [{**restart-interval** | **helper** [{**disable** | **strict-lsa-checking**}]}]

Syntax Description

restart-interval *seconds*	(Optional) Specifies length of the graceful restart interval, in seconds. The range is from 1 to 1800. The default is 120.
helper	(Optional) Configures NSF helper mode.
disable	(Optional) Disables helper mode on an NSF-aware router.
strict-lsa-checking	(Optional) Enables strict link-state advertisement (LSA) checking for helper mode.

Command Default

IETF NSF graceful restart mode is disabled. IETF NSF helper mode is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command enables IETF NSF on an OSPF router. When NSF is enabled on a Cisco router, the router is NSF-capable and will operate in restarting mode.

If a router is expected to cooperate with a neighbor that is doing an NSF graceful restart only, the neighbor router must be running a Cisco software release that supports NSF but NSF need not be configured on the router. When a router is running a Cisco software release that supports NSF, the router is NSF-aware.

By default, neighboring NSF-aware routers will operate in NSF helper mode during a graceful restart. To disable IETF NSF helper mode on an NSF-aware router, use this command with the **disable** keyword. To reenable helper mode after explicitly disabling helper mode on an NSF-aware router, use the **no nsf ietf helper disable** command.

Strict LSA checking allows a router in IETF NSF helper mode to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. You can configure strict LSA checking on NSF-aware and NSF-capable routers but it is effective only when the router is in helper mode.

Examples

The following example enables IETF NSF restarting mode on a router and changes the graceful restart interval from default (120 seconds) to 200 seconds:

```
router ospf 24
 nsf ietf restart-interval 200
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF.

nsf interface wait

To specify how long a Cisco nonstop forwarding (NSF) restart will wait for all interfaces with Intermediate System-to-Intermediate System (IS-IS) adjacencies to come up before completing the restart, use the **nsf interface wait**command in router configuration IS-IS 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.

nsf interface wait *seconds*
no nsf interface wait *seconds*

Syntax Description

seconds	The valid range is from 1 to 60 seconds.

Command Default

The default value for the *seconds* argument is 10.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support for the Cisco 7304 router was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **nsf interface wait** command can be used if Cisco proprietary IS-IS NSF is configured or if Internet Engineering Task Force (IETF) IS-IS NSF is enabled using the **nsf t3 manual**command. You can use this command if an interface is slow to come up.

Examples

The following example specifies that NSF restart will wait 15 seconds for all interfaces with IS-IS adjacencies to come up before completing the restart:

```
Router(config)# router isis
Router(config-router)# nsf cisco
Router(config-router)# nsf interface wait 15
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interval	Specifies the minimum time between NSF restart attempts.

Command	Description
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
show clns neighbors	Displays both ES and IS neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf interval

To configure the minimum time between Cisco nonstop forwarding (NSF) restart attempts, use the **nsf interval**command in router configuration Intermediate System-to-Intermediate System (IS-IS) 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.

nsf interval *minutes*
no nsf interval *minutes*

Syntax Description

minutes	The length of time in minutes between restart attempts. The valid range is from 0 to 1440 minutes.

Command Default

The default value for the *minutes* argument is 5.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support for the Cisco 7304 router was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **nsf interval** command can be used with both Cisco proprietary IS-IS NSF and Internet Engineering Task Force (IETF) IS-IS NSF. When you use Cisco proprietary IS-IS NSF, the active route processor (RP) must be up for at least 5 minutes before IS-IS will attempt to perform an NSF restart as part of a stateful switchover.

When you use the **nsf** command with the **ietf**keyword, the standby RP must be up for at least 5 minutes before IS-IS will attempt to perform an NSF restart as part of a stateful switchover.

Examples

The following example configures the minimum time between NSF restart attempts to be 2 minutes:

```
Router(config-router)# router isis
Router(config-router)# nsf cisco
Router(config-router)# nsf interval 2
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.

Command	Description
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
show clns neighbors	Displays both IS and ES neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf t3

To specify the methodology used to determine how long Internet Engineering Task Force (IETF) Cisco nonstop forwarding (NSF) will wait for the link-state packet (LSP) database to synchronize before generating overloaded link-state information for itself and flooding that information out to its neighbors, use the **nsf t3**command in router configuration IS-IS 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.

nsf t3 {**manual** *seconds* | **adjacency**}
no nsf t3 {**manual** *seconds* | **adjacency**}

Syntax Description

manual *seconds*	The amount of time (in seconds) that IETF NSF waits for the LSP database to synchronize is set manually by the user. The range is from 5 to 3600 seconds.
adjacency	The time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover.

Command Default

The default value for the *seconds* argument is 30.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support for the Cisco 7304 router was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When the **nsf t3 adjacency** command is enabled, the time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover. When the **nsf t3 manual** command is enabled, the specified time in seconds is used.

The **nsf t3 manual** command can be used only if IETF IS-IS NSF is configured.

Examples

In the following example, the amount of time that IETF NSF waits for the LSP database to synchronize is set to 40 seconds:

```
nsf t3 manual 40
```

In the following example, the amount of time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover:

```
nsf t3 adjacency
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf interval	Specifies the minimum time between NSF restart attempts.
show clns neighbors	Displays both IS and ES neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

phone-number

To assign the phone number to be used for customer contact for Call Home, use the **phone-number** command in call home configuration mode. To remove the phone number, use the **no** form of this command.

phone-number *+phone-number*
no phone-number *+phone-number*

Syntax Description

phone-number	12 to16 digits (not including the plus (+) prefix), using hyphens (-) or spaces, and numbers. If you include spaces, you must enclose your entry in quotes (“ ”).

Command Default

No phone number is assigned for customer contact.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **phone-number** command is optional.

Examples

The following example shows how to configure the phone number 1-222-333-444 for customer contact without dashes or spaces:

```
Router(config)# call-home
Router(cfg-call-home)# phone-number +12223334444
```

The following example shows how to configure the same phone number for customer contact using hyphens:

```
Router(config)# call-home
Router(cfg-call-home)# phone-number +1-222-333-4444
```

The following example shows how to configure the same phone number for customer contact using spaces:

```
Router(config)# call-home
Router(cfg-call-home)# phone-number "+1 222 333 4444"
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.

show call-home	Displays call home configuration information.

platform redundancy bias

To configure the standby slot Supervisor (SUP) bootup delay time, use the platform redundancy bias command in global configuration mode.

platform redundancy bias *seconds*

Syntax Description

seconds	Delay time in seconds. The range is from 1 to 3600.

Command Default

The command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
12.2(33)SRD4	This command was integrated into Cisco IOS Release 12.2(33)SRD4.

Usage Guidelines

The slave slot SUP, on certain occasions, boots up faster than the master slot SUP, thereby becoming active. The **platform redundancy bias** command allows you to configure the delay in bootup time such that the slave slot SUP always boots up slower than the master slot SUP, and does not become active.

Examples

The following example shows how to configure the standby slot SUP bootup delay setting for 25 seconds:

```
Device# configure terminal
Device(config)# platform redundancy bias 25
Device(config)# end
```

Related Commands

Command	Description
show platform redundancy bias	Displays the output for a specific **platform redundancy bias** command.

policy config-sync reload

To enable and specify configuration synchronization policy during a reload between active and standby route processor (RP) modules, use the **policy config-sync reload** command in global configuration mode or in redundancy configuration mode. To disable the configuration synchronization policy and to return to the default setting, use the **no** form of this command.

policy config-sync {**bulk** | **lbl**} {**bem** | **prc**} **reload**
no policy config-sync {**bulk** | **lbl**} {**bem** | **prc**} **reload**

Syntax Description

bulk	Specifies bulk synchronization.
lbl	Specifies line-by-line (lbl) synchronization.
bem	Specifies the best effort method for the configuration synchronization policy.
prc	Specifies the parser return code method for the configuration synchronization policy.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config) #

Redundancy configuration (config-red) #

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2SR	This command was modified. This command was made available in redundancy configuration mode.
15.1S	This command was integrated into Cisco IOS Release 15.1S. This command was made available in redundancy configuration mode.

Examples

The following example shows how to enable and specify the configuration synchronization policy during the reload between active and standby RP modules:

```
Device# configure terminal
Device(config)# redundancy configuration
Device(config-red)# policy config-sync bulk reload
```

Related Commands

Command	Description
show mdr	Displays the minimal disruption restart (MDR) state machine status.

profile (call home)

To configure a destination profile to specify how alert notifications are delivered for Call Home and enter call home profile configuration mode, use the **profile (call home)** command in call home configuration mode. To delete a named destination profile or all destination profiles, use the **no** form of this command.

The CiscoTAC-1 predefined profile will be reset to its default configuration when using the no form of the command. (**no profile CiscoTAC-1**)

profile *profile-name*
no profile {*profile-name* | **all**}

Syntax Description

profile-name	Name of the destination profile.
all	Removes all user-defined destination profiles and reset CiscoTAC-1 profile to default.

Command Default

After you configure a destination profile, the profile is automatically enabled for Call Home. This does not apply to the CiscoTAC-1 predefined profile.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When you enter the **profile (call home)** command, you enter call home profile configuration mode to specify how alert notifications are delivered for Call Home. Some of the available call home profile configuration commands are shown in the Examples section.

After you configure a profile, it is automatically enabled for use by Call Home. If you do not want the profile to be active in the Call Home configuration, use the **no active** command. You can reactivate the profile using the **active** command.

The predefined CiscoTAC-1 profile is disabled by default.

Examples

The following example shows how to enter call home profile configuration mode:

```
Router(conf)# call-home
Router(cfg-call-home)# profile example
Router(cfg-call-home-profile)#?
Call-home profile configuration commands:
  active                   Activate the current profile
  default                  Set a command to its defaults
```

```
destination               Message destination related configuration
exit                      Exit from call-home profile configuration mode
no                        Negate a command or set its defaults
subscribe-to-alert-group  Subscribe to alert-group
```

Related Commands

active (call home)	Enables a destination profile for Call Home.
call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
destination (call home)	Configures the message destination parameters for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.
subscribe-to-alert-group all	Configures a destination profile to receive messages for all available alert groups for Call Home.
subscribe-to-alert-group configuration	Configures a destination profile to receive messages for the Configuration alert group for Call Home.
subscribe-to-alert-group diagnostic	Configures a destination profile to receive messages for the Diagnostic alert group for Call Home.
subscribe-to-alert-group environment	Configures a destination profile to receive messages for the Environment alert group for Call Home.
subscribe-to-alert-group inventory	Configures a destination profile to receive messages for the Inventory alert group for Call Home.
subscribe-to-alert-group syslog	Configures a destination profile to receive messages the Syslog alert group for Call Home.

profile (diagnostic signature)

To specify a destination profile that a diagnostic signature uses on a device, use the **profile** command in call-home diagnostic-signature configuration mode. To set a default profile, use the **no** or the **default** form of this command.

profile *ds-profile-name*
no profile
default profile

Syntax Description

ds-profile-name	Destination profile that the diagnostic signature uses.

Command Default

The CiscoTAC-1 profile is used as diagnostic signature destination profile.

Command Modes

Call-home diagnostic-signature configuration (cfg-call-home-diag-sign)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

You can specify the destination profile name that the diagnostic signature feature will use. To download diagnostic signature files, the specified profiles must be active, have HTTP(s) as transport method, and have at least one HTTP destination URL configured.

In call-home profile configuration mode, use the **active** command to activate a specified profile. Use the **destination transport-method** command to define a destination transport method. Use the **destination address http** command to add a destination address.

Example

The following example shows how to activate profile prof-1 and specify HTTP as the profile destination transport method:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# profile prof-1
Device(cfg-call-home-profile)# active
Device(cfg-call-home-profile)# destination transport-method http
Device(cfg-call-home-profile)# end
```

The following example shows how to specify profile prof-1 defined in the previous example to be used by the diagnostic signature:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# profile prof-1
Device(cfg-call-home-diag-sign)# end
```

Related Commands

Command	Description
active (diagnostic signature)	Activates diagnostic signature on a device.
call-home	Enters call-home configuration mode.
destination-address	Configures the address type and the location to which call-home messages are sent.
destination transport-method	Specifies the transport method for a call-home profile.
diagnostic-signature	Enters call-home diagnostic-signature configuration mode.

rate-limit (call home)

To configure the maximum number of messages per minute for Call Home, use the **rate-limit (call home)**command in call home configuration mode. To return to the default, use the **no** form of this command.

rate-limit *threshold*
no rate-limit [*threshold*]

Syntax Description

threshold	Maximum number of messages per minute from 1 to 60. The default is 20.

Command Default

If the **rate-limit (call home)** command is not configured, the maximum number of messages per minute is 20.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **rate-limit (call home)**command is optional.

Examples

The following example changes the call home maximum message rate to 50 messages per minute:

```
Router(config)# call-home
Router(cfg-call-home)# rate-limit 50
```

The following example changes the call home maximum message rate back to 20 messages per minute:

```
Router(cfg-call-home)# no rate-limit
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
show call-home	Displays Call Home configuration information.

redundancy

To enter redundancy configuration mode, use the **redundancy**command in global configuration mode. This command does not have a **no** form.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Release	Modification
12.2(33) SRE	This command was modified. The interchassis subconfiguration mode was added.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.
- Define the peer monitoring method using the **monitor** command.

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

Examples

The following example shows how to enable redundancy mode:

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

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router(config)#
redundancy
Router(config-r)#
main-cpu
Router(config-r-mc)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
```

```
Router(config)# redundancy

Router(config-r)# ?

Redundancy configuration commands:
  associate  Associate redundant slots
  exit       Exit from redundancy configuration mode
  main-cpu   Enter main-cpu mode
  no         Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?
Redundancy configuration commands:
  default         Set a command to its defaults
  exit            Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu        Enter main-cpu mode
  mode            redundancy mode for this chassis
  no              Negate a command or set its defaults
  policy          redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
```

Router(config-r)#?

```
Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults
Router(config-r)# interchassis group 100

R1(config-r-ic)# ?
Interchassis redundancy configuration commands:
  backbone  specify a backbone interface for the redundancy group
  exit      Exit from interchassis configuration mode
  member    specify a redundancy group member
  mlacp     mLACP interchassis redundancy group subcommands
  monitor   define the peer monitoring method
  no        Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.

Command	Description
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers. In the redundancy configuration of Cisco ASR 920 Series Routers, the commands related to MR-APS feature are only supported.

redundancy config-sync

To ignore mismatched commands between active and standby Route Processor (RP) modules, use the **redundancy config-sync** command in privileged EXEC mode to temporarily ignore the mismatched commands that are not supported on the standby RP module.

redundancy config-sync {**ignore** | **validate**} **mismatched-commands**

Syntax Description

ignore	Ignores mismatched commands.
validate	Validates mismatched commands against commands in the running-config file.
mismatched-commands	Validates or ignores mismatched commands across active and standby RP modules.

Command Default

All mismatched commands are validated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following is sample output from the **redundancy config-sync** command:

```
Device# redundancy config-sync ignore mismatched-commands

.
.
.
MCL validation succeeded.
```

Related Commands

Command	Description
show redundancy config-sync	Displays failure information generated during a bulk synchronization from the active RP module to the standby RP module.

redundancy force-switchover

To force the standby Route Processor (RP) or Supervisor card to assume the role of the active RP or Supervisor card, use the **redundancy force-switchover** command in privileged EXEC mode.

redundancy force-switchover [**main-cpu**]

Syntax Description

main-cpu	(Optional) Forces switchover to the main CPU.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.1(10)EX2	This command was integrated into Cisco IOS Release 12.1(10)EX2.
12.0(17)ST	This command was implemented on the Cisco 12000 series routers.
12.0(22)S	This command replaces the **force-failover**command on the Cisco 10000 series routers.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series routers.
12.2(20)S	Support was added for the Cisco 7304 router.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Usage Guidelines

Use the **redundancy force-switchover** command to switch control of a router from the active RP or Supervisor card to the standby RP or Supervisor card. Both the active and standby RPs or Supervisor cards must have a high availability Cisco IOS image installed and must be configured for Route Processor Redundancy (RPR) mode before the **redundancy force-switchover** command can be used. Before the system switches over, it verifies that the standby RP or Supervisor card is ready to take over.

When you use the **redundancy force-switchover**command and the current running configuration is different from the startup configuration, the system prompts you to save the running configuration before the switchover is performed.

Note All line cards will reset in RPR mode on a switchover.

Note Before using this command in Cisco 7600 series routers, refer to the "Performing a Fast Software Upgrade" section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guid*e for additional information.

On Cisco 7600 series routers, the **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the new Cisco IOS image. The modules are reset and the module software is downloaded from the new active supervisor engine.

The active and redundant supervisor engines do not reset on a Route Processor Redundancy Plus (RPR+) switchover. The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine.

Beginning with Cisco IOS Release 12.2(33)SCA, you can force a Performance Routing Engine (PRE) switchover using the **redundancy force-switchover main-cpu** command from either the primary or standby PRE. If you force a switchover from the active PRE, both PREs synchronize and the active PRE reloads normally. When you force a switchover from the standby PRE, a crash dump of the active PRE occurs for troubleshooting purposes. Forcing a switchover from the standby PRE should only be done if you cannot access the active PRE.

Examples

The following example shows a switchover from the active RP to the standby RP on a Cisco 7513 router with RPR configured:

```
Router# configure terminal
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# slave auto-sync config
Router(config)# redundancy
Router(config-r)# mode rpr
Router(config-r)# end
Router# copy running-config startup-config
Router# redundancy force-switchover
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover
System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover
Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Cisco RF Gateway 10

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover
System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover
Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
hw-module sec-cpu reset	Resets and reloads the standby RP with the specified Cisco IOS image and executes the image.
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RP.
mode (HSA redundancy)	Configures the High System Availability (HSA) redundancy mode.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy	Enters redundancy configuration mode.
show redundancy	Displays current active and standby Performance Routing Engine (PRE) redundancy status.

redundancy reload peer

To reload a standby Route Processor (RP) module, use the **redundancy reload peer** command in privileged EXEC mode.

redundancy reload peer

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

The **redundancy reload peer** command is used to reset standby RP module when there are any failures, tracebacks, or functionality and behavior mismatches on either one or both active and standby RP modules.

This command does not have an impact on active device operations, assuming a switchover is not required while the standby module is resetting.

Examples

The following example shows how to manually reload the standby RP module:

```
Device# redundancy reload peer
Reload peer? [confirm] y
Preparing to reload peer
```

Note Pressing **enter** or **y** begins the reload. Pressing any other key aborts the reload and returns control to the active RP module.

The following is sample output when a standby RP module is not installed on a router:

```
Device# redundancy reload peer
System is running in SIMPLEX mode, reload anyway? [confirm] n
Peer reload not performed.
```

Related Commands

Command	Description
associate slot	Associates slots for APS processor redundancy.
redundancy	Enters redundancy configuration mode so that the synchronization parameters can be configured.
redundancy force-failover main-cpu	Forces a switchover so that the standby RP module becomes the active RP module.
redundancy switch-activity	Forces a switchover to the standby RP module.

rename profile

To change the name of a destination profile, use the **rename profile** command in call home configuration mode.

rename profile *source-profile target-profile*

Syntax Description

source-profile	Name of the existing destination profile that you want to rename.
target-profile	New name of the destination profile.

Command Default

This command has no default behavior or values.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **rename profile** command when you want to change the name of an existing destination profile for Call Home.

Examples

The following example changes the name of “profile2” to “testprofile”:

```
Router(config)# call-home
Router(cfg-call-home)# rename profile profile2 testprofile
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
profile (call home)	Configures a destination profile to specify how alert notifications are delivered for Call Home and enters call home profile configuration mode.
show call-home	Displays Call Home configuration information.

request platform software package verify rp file

To verify the ISSU compatibility between the current and the target image, use the request platform software package verify rp file command in privileged EXEC mode.

Using the mdr as a keyword, you can also verify the Minimal Disruptive Restart (MDR) compatibility.

request platform software package verify rp *slot* **file** *URL***[mdr | force**

Syntax Description

slot	Route processor slot number.
URL	URL to the file. The URL contains the name of the file system, directories, and filename.
mdr	Specifies the setting for MDR upgrade process.
force	Specifies that the operation will be forced, meaning the upgrade will proceed despite warning messages, if any.

Command Default

This command is disabled by default

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced in the Cisco ASR 1000 Series Aggregation Services Routers.

Example

The following is sample output from the request platform software package verify command is used to verify the mdr upgrade compatibility in a consolidated package or subpackage running on RP 1:

```
Router# request platform software package verify rp 1 file
stby-harddisk:RP2_XE38_20121101_080017_iso1 mdr

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

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

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

--- Starting file path checking ---
Finished file path checking

--- Starting system installation readiness checking ---
Finished system installation readiness checking

--- Starting image verification ---
Compatibility check with running software on active RP
```

```
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Software sets are identified as compatible
Finished image verification

--- Starting mdr compatibility verification ---
Extracting consolidated package content
Checking and verifying packages contained in consolidated package
Creating candidate provisioning file
Processing candidate provisioning file

WARNING:

MDR for SPA type [0x43B] located at slot [5] bay [2] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]

WARNING:

FAILED: MDR compatibility failed - alternatively run with 'force' option to proceed. However
 not all FRU's may be upgraded using MDR.
```

The fields shown in the display are self-explanatory.
The following is sample output from the request platform software package verify command is used to verify the mdr upgrade compatibility in a consolidated package or subpackage running on RP 1. The force option, which forces the upgrade past any prompt (such as already having the same consolidated package installed), is used in this example.

```
Router# request platform software package verify rp 1 file
stby-harddisk:RP2_XE38_20121101_080017_iso1 mdr force
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

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

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

--- Starting file path checking ---
Finished file path checking

--- Starting system installation readiness checking ---
Finished system installation readiness checking

--- Starting image verification ---
Compatibility check with running software on active RP

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Software sets are identified as compatible
Finished image verification

--- Starting mdr compatibility verification ---
Extracting consolidated package content
Checking and verifying packages contained in consolidated package
Creating candidate provisioning file
Processing candidate provisioning file


WARNING:
```

```
MDR for SPA type [0x55E] located at slot [2] bay [2] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]

WARNING:

MDR for SPA type [0x43F] located at slot [3] bay [1] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]


WARNING:

MDR for SPA type [0x43B] located at slot [5] bay [2] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]

WARNING:

MDR compatibility failed - proceeding with forced MDR-upgrade - some traffic will be impacted
 during the upgrade
Finished mdr compatibility verification

SUCCESS: Software is ISSU MDR compatible.
```

The fields shown in the display are self-explanatory.

Related Commands

Command	Description
request platform software package install file	Upgrades an individual package file or a consolidated package file.

sender

To assign the e-mail addresses to be used in the from and reply-to fields in messages for Call Home, use the **sender** command in call home configuration mode. To remove the assigned e-mail addresses, use the **no** form of this command.

sender {**from** | **reply to**}*email-address*
no sender {**from** | **reply to**}*email-address*

Syntax Description

from	Assigns the specified e-mail address to appear in the "from" field in Call Home e-mail messages.
reply-to	Assigns the specified e-mail address to appear in the "reply-to" field in Call Home e-mail messages.
email-address	Up to 200 characters in standard e-mail address format (contactname@domain) with no spaces.

Command Default

If the **sender from** command is not configured, the address specified in the **contact-email-addr**command for Call Home is used for all destination profiles. There is no default value for the **reply-to** option.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **sender** command is optional.

Examples

The following example configures the e-mail address "username@example.com" to appear in the from field of Call Home messages:

```
Router(config)# call-home
Router(cfg-call-home)# sender from username@example.com
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
contact-email-addr	Assigns the e-mail address to be used for customer contact for Call Home.

show call-home	Displays Call Home configuration information.

service call-home

To enable Call Home, use the **service call-home** command in global configuration mode. To disable the Call Home, use the **no** form of this command.

service call-home
no service call-home

Syntax Description

This command has no arguments or keywords.

Command Default

Call Home is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

The following example shows how to enable Call Home:

```
Router(config)# service call-home
```

The following example shows how to disable Call Home:

```
Router(config)# no service call-home
```

Related Commands

Command	Description
call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
call-home test	Manually sends a Call Home test message to a destination profile.
show call-home	Displays Call Home configuration information.

service image-version compatibility

To enable Fast Software Upgrade (FSU) functionality, use the **service image-version compatibility**command in global configuration mode. To omit the compatibility matrix and enable Enhanced Fast Software Upgrade (eFSU) functionality, use the no form of this command.

service image-version compatibility
no service image-version compatibility

Syntax Description

This command has no arguments or keywords.

Command Default

Fast Software Upgrade (FSU) is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	Enhanced Fost Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. In Service Software Upgrade (ISSU) is not supported in the 12.2(33)SRB release.

Usage Guidelines

Use the **service image-version compatibility**command to enable FSU, and use the no **service image-version compatibility**command to omit the compatibility matrix and enable eFSU functionality.

Examples

The following example enables eFSU functionality:

```
Router(config)# no service image-version compatibility
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
service image-version efsu	Enables eFSU functionality.

service image-version efsu

To enable Enhanced Fast Software Upgrade (eFSU) functionality, use the **no** version of the **service image-version efsu**command in global configuration mode.

no service image-version efsu

Syntax Description

This command has no arguments or keywords.

Command Default

eFSU functionality is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The **no service image-version efsu** command functionality is similar to that of the **service image-version compatibility** command. The **no service image-version efsu** command is used to omit the compatibility matrix creation for Cisco 7600 series router eFSU images.

Examples

The following example enables eFSU functionality:

```
Router# no service image-version efsu
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
service image-version compatibility	Enables FSU functionality.