HA Command Reference

First Published: February 21, 2012

Last Modified: February 21, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

A through L

active (call home)

To enable a destination profile for Call Home, use the active command in call home profile configuration mode. To disable a profile, use the **no** form of the command. To enable a user-defined profile, use the **default** form of the command, or to disable the CiscoTac-1 predefined profile, use the **default** form of the command.

active

no active

default active

Syntax Description

This command has no arguments or keywords.

Command Default

A user-defined destination profile is automatically enabled in Call Home after it is created. The predefined CiscoTac-1 profile is disabled.

Command Modes

Call home profile configuration (cfg-call-home-profile)

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS XE 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

A destination profile in Call Home is enabled when it is created. To disable a profile, use the **no active** command.

Examples

The following shows how to disable a destination profile that is automatically activated upon creation:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# no
 active
```

The following shows how to reactivate a destination profile that is disabled:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# active
```

Related Commands

Command	Description
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.

alert-group

To enable an alert group, use the **alert-group** command in call home configuration mode. To disable an alert group, use the **no** form of this command.

alert-group {**all**| **configuration**| **diagnostic**| **environment**| **inventory**| **syslog**}

no alert-group

Syntax Description

all	Specifies all the alert groups.
configuration	Specifies the configuration alert group.
diagnostic	Specifies the diagnostic alert group.
environment	Specifies the environmental alert group.
inventory	Specifies the inventory alert group.
syslog	Specifies the syslog alert group.

Command Default

All alert groups are enabled.

Command Modes

Call home configuration (cfg-call-home)

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

An *alert group* is a predefined subset of Call Home alerts supported on a platform. Different types of Call Home alerts are grouped into different alert groups depending on their type. The alert are as follows:

- Configuration
- Diagnostic
- Environment
- Inventory
- Syslog

Note The diagnostic alert group is not supported in Cisco IOS Release 12.4(24)T.

Call Home trigger events are grouped into alert groups with each alert group assigned command-line interface commands to execute when an event occurs. These alert group trigger events and executed commands are platform-dependent. For more information, see the platform-specific configuration guides on the Smart Call Home site on Cisco.com at:

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Examples

The following example shows how to enable a specific alert group:

```
Router(config)# call-home
Router(cfg-call-home)# alert-group configuration
```

The following example shows how to enable all alert groups:

```
Router(cfg-call-home)# alert-group all
```

The following example shows how to disable a specific alert group:

```
Router(cfg-call-home)# no alert-group syslog
```

The following example shows how to disable all alert groups:

```
Router(cfg-call-home)# no alert-group all
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
show call-home	Displays call home configuration information.

call-home (global configuration)

To enter call home configuration mode for configuration of Call Home settings, use the **call-home (global configuration)** command in global configuration mode.

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

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 use the **call-home** command, you enter call home configuration mode and can configure settings for the Call Home feature. Some of the available call home configuration commands are shown in the Examples section.

Examples

The following example shows how to enter call home configuration mode and lists the commands that are available for Call Home configuration in Cisco IOS XE Release 2.6:

```
Router(config)# call-home

Router(cfg-call-home)#?
Call-home configuration commands:
  alert-group         Enable or disable alert-group
  contact-email-addr  System Contact's email address
  contract-id         Contract identification for Cisco AutoNotify
  copy                Copy a call-home profile
  customer-id         Customer identification for Cisco AutoNotify
  default             Set a command to its defaults
```

```
exit                Exit from call-home configuration mode
mail-server         Configure call-home mail_server
no                  Negate a command or set its defaults
phone-number        Phone number of the contact person
profile             Enter call-home profile configuration mode
rate-limit          Configure call-home message rate-limit threshold
rename              Rename a call-home profile
sender              Call home msg's sender email addresses
site-id             Site identification for Cisco AutoNotify
street-address      Street address for RMA part shipments
vrf                 VPN Routing/Forwarding instance name
```

Related Commands

Command	Description
alert-group	Enables an alert group.
contact-email-addr	Assigns the e-mail address to be used for customer contact for Call Home.
contract-id	Assigns the customer's contract identification number for Call Home.
copy profile	Creates a new destination profile with the same configuration settings as an existing profile.
customer-id (call home)	Assigns a customer identifier for Call Home.
mail-server	Configures an SMTP e-mail server address for Call Home.
phone-number	Assigns the phone number to be used for customer contact for Call Home.
profile (call home)	Configures a destination profile to specify how alert notifications are delivered for Call Home and enters call home profile configuration mode.
rate-limit (call home)	Configures the maximum number of messages per minute for Call Home.
rename profile	Changes the name of a destination profile.
sender	Assigns the e-mail addresses to be used in the from and reply-to fields in messages for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.
site-id	Assigns a site identifier for Call Home.
street-address	Specifies a street address where RMA equipment for Call Home can be sent.

Command	Description
vrf (call home)	Associates a VRF instance for Call Home e-mail message transport.

call-home send alert-group

To manually send an alert group message for the Call Home feature, use the **call-home send alert-group** command in privileged EXEC mode.

Cisco Catalyst 6500 Series Switches, Cisco Catalyst 4500 Series Switches, Cisco 7600 Series Routers

call-home send alert-group {**configuration**| **diagnostic module** *number*| **inventory**} [**profile** *profile-name*]

Cisco ASR 1000 Series Aggregation Services Routers

call-home send alert-group {**configuration**| **diagnostic slot** *number*| **inventory**} [**profile** *profile-name*]

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
diagnostic module *number*	(Cisco Catalyst 6500 series switches, Cisco Catalyst 4500 series switches, and Cisco 7600 series souters) Sends the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay number. This option is not supported on the Cisco ASR 1000 Series Router.
inventory	Sends the inventory call-home message.
profile *profile-name*	(Optional) Specifies the name of the destination profile.
diagnostic slot *number*	(Cisco ASR 1000 Series Routers) Sends the diagnostic alert-group message to destination profiles for the specified slot, such as R0 for Route Processor slot 0.

Command Default

A Call Home alert group message is not manually sent.

Command Modes

Privileged EXEC (#)

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.

Release	Modification
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. The **diagnostic slot R0** keyword option was added.

Usage Guidelines

When you enter the module number, you can enter the number of the module, the slot/subslot, or the slot/bay number.

Note The Cisco ASR 1000 Series Router does not support the **module** keyword option. Instead, use the **slot** keyword.

If you do not specify the **profile***profile-name*, the message is sent to all subscribed destination profiles. If you do specify a profile, the destination profile does not need to be subscribed to the alert group.

Only the configuration, diagnostic, and inventory alert groups can be manually sent.

Examples

The following example shows how to send the configuration alert-group message to the destination profile:

```
Router# call-home send alert-group configuration
```

The following example shows how to send the diagnostic alert-group message to all subscribed destination profiles that have lower severity subscription than the diagnostic result for a specific module, slot/subslot, or slot/bay number:

```
Router# call-home send alert-group diagnostic module 3/2
```

The following example shows how to send the diagnostic alert-group message to the destination profile named CiscoTAC-1 for a specific module, slot/subslot, or slot/bay number:

```
Router# call-home send alert-group diagnostic module 3/2 profile CiscoTAC-1
```

The following example shows how to send the diagnostic alert-group message to the destination profile named CiscoTAC-1 on RP slot 0 on a Cisco ASR 1000 Series Router:

```
Router# call-home send alert-group diagnostic slot R0 profile CiscoTAC-1
```

The following example shows how to send an inventory call-home message to the destuination profile:

```
Router# call-home send alert-group inventory
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home test	Manually sends a Call Home test message to a destination profile.
service call-home	Enables Call Home.

show call-home	Displays Call Home configuration information.

configure issu set rollback timer

To configure the rollback timer value, use the **configure issu set rollback timer** command in global configuration mode.

configure issu set rollback timer *seconds*

Syntax Description

seconds	The rollback timer value, in seconds. The valid timer value range is from 0 to 7200 seconds (two hours). A value of 0 seconds disables the rollback timer.

Command Default

Rollback timer value is 45 minutes.

Command Modes

Global configuration (config)

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. In Service Software Upgrade (ISSU) is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the configure issue set rollback timer command to configure the rollback timer value. Note that you can enable this command only when the Route Processors (RPs) are in the init state.

Examples

The following example sets the rollback timer value to 3600 seconds, or 1 hour:

```
Router(config)# configure issu set rollback timer 3600
```

Related Commands

Command	Description
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
show issu rollback timer	Displays the current setting of the ISSU rollback timer.

contact-email-addr

To assign the e-mail address to be used for customer contact for Call Home, use the **contact-email-addr** command in call home configuration mode. To remove the assigned e-mail address, use the **no** form of this command.

contact-email-addr *email-address*

no contact-email-addr *email-address*

Syntax Description

email-address	Up to 200 characters in standard e-mail address format (contactname@domain) with no spaces.

Command Default

No e-mail address is assigned for customer contact.

Command Modes

Call home configuration (cfg-call-home)

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

To support the Call Home feature, the **contact-email-addr** command must be configured.

Examples

The following example configures the e-mail address “username@example.com” for customer contact:

```
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
```

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.

contract-id

To assign the customer's contract identification number for Call Home, use the **contract-id** command in call home configuration mode. To remove the contract ID, use the **no** form of this command.

contract-id *alphanumeric*

no contract-id *alphanumeric*

Syntax Description

alphanumeric	Contract number, using up to 64 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").

Command Default

No contract ID is assigned.

Command Modes

Call home configuration (cfg-call-home)

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

You must have a service contract for your Cisco device to use the Smart Call Home service. You can specify this contract number in the Call Home feature using the **contract-id (call home)** command.

Examples

The following example configures "Company1234" as the customer contract ID:

```
Router(config)# call-home
Router(cfg-call-home)# contract-id Company1234
```

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.

copy profile

To create a new destination profile with the same configuration settings as an existing profile, use the **copy profile** command in call home configuration mode.

copy profile *source-profile target-profile*

Syntax Description

source-profile	Name of the existing destination profile that you want to copy.
target-profile	Name of the new destination profile that you want to create from the copy.

Command Default

No default behavior or values.

Command Modes

Call home configuration (cfg-call-home)

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

To simplify configuration of a new profile, use the **copy profile** command when an existing destination profile has configuration settings that you want to use as a basis for a new destination profile.

After you create the new profile, you can use the **profile (call home)** command to change any copied settings that need different values.

Examples

The following example creates a profile named “profile2” from an existing profile named “profile1”:

```
Router(config)# call-home
Router(cfg-call-home)# copy profile profile1 profile2
```

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.

customer-id (call home)

To assign a customer identifier for Call Home, use the **customer-id** command in call home configuration mode. To remove the customer ID, use the **no** form of this command.

customer-id *alphanumeric*

no customer-id *alphanumeric*

Syntax Description

alphanumeric	Customer identifier, using up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).

Command Default

No customer ID is assigned.

Command Modes

Call home configuration (cfg-call-home)

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 **customer-id** command is optional.

Examples

The following example configures “Customer1234” as the customer ID:

```
Router(config)# call-home
Router(cfg-call-home)# customer-id Customer1234
```

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.

debug atm ha-events

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

debug atm ha-events[detailed]

no debug atm ha-events[detailed]

Syntax Description

detailed	(Optional) Displays detailed output.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S on Cisco 7500 series routers.
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.
XE 3.6S	This command was modified. The **detailed** keyword was added.

Examples

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

```
Router# debug atm ha-events
```

Related Commands

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

debug frame-relay redundancy

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

debug frame-relay redundancy

no debug frame-relay redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Release	Modification
12.0(22)S	This command was introduced on the Cisco 7500 series and Cisco 10000 series Internet routers.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S on Cisco 7500 series routers.
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.
12.0(28)S	SSO support was added to the Multilink Frame Relay feature on the Cisco 12000 series Internet router.
12.2(25)S	SSO support was added to the Multilink Frame Relay feature on the Cisco 12000 series Internet router.
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

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

Examples

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

```
Router# debug frame-relay redundancy
```

Related Commands

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

debug ip bgp vpnv4 nsf

To display the nonstop forwarding events for the VRF table-id synchronization subsystem between the active and standby Route Processors, use the debug ip bgp vpnv4 nsf command in privileged EXEC mode. To disable the display of these events, use the **no** form of this command.

debug ip bgp vpnv4 nsf

no debug ip bgp vpnv4 nsf

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
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.

Examples

The following example shows the command output on the active Route Processor:

```
Router# debug ip bgp vpnv4 nsf
MPLS VPN NSF Processing debugging is on
Router(config)# ip vrf vpn3
3d18h: vrf-nsf: vrf vpn3 tableid 2 send rpc OK
Router(config-vrf)# no ip vrf vpn3
% IP addresses from all interfaces in VRF vpn3 have been removed
3d18h: vrf-nsf:  rx vrf tableid delete complete msg, tid = 2, name = vpn3
```

The following example shows the command output on the standby Route Processor:

```
Router# debug ip bgp vpnv4 nsf
MPLS VPN NSF Processing debugging is on
00:05:21: vrf-nsf: rx vrf tableid rpc msg, tid = 2, name = vpn3
% IP addresses from all interfaces in VRF vpn3 have been removed
00:06:22: vrf-nsf: vrf vpn3 tableid 2 , delete complete, send OK
```

Related Commands

Command	Description
debug ip bgp vpnv4 checkpoint	Display the events for the VRF checkpointing system between the active and standby Route Processors.

debug isis nsf

To display information about the Intermediate System-to-Intermediate System (IS-IS) state during a Cisco nonstop forwarding (NSF) restart, use the **debug isis nsf** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug isis nsf [detail]

no debug isis nsf [detail]

Syntax Description

detail	(Optional) Provides detailed debugging information.

Command Modes

Privileged EXEC

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

Use the **debug isis nsf** command to display basic information about the IS-IS state during an NSF restart. Use the **debug isis nsf detail** command to display additional IS-IS state detail during an NSF restart.

Examples

The following example displays IS-IS state information during an NSF restart:

```
router# debug isis nsf
IS-IS NSF events debugging is on
```

The following example displays detailed IS-IS state information during an NSF restart:

```
router# debug isis nsf detail
IS-IS NSF events (detailed) debugging is on
router#
```

```
Jan 24 20:04:54.090:%CLNS-5-ADJCHANGE:ISIS:Adjacency to gsr1 (GigabitEthernet2/0/0) Up,
Standby adjacency
Jan 24 20:04:54.090:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/1, cnt 0/1, ht 10 (NEW)
Jan 24 20:04:54.142:ISIS-NSF:Rcv LSP - L2 000B.0000.0000.00-00, seq 251, csum B0DC, ht 120,
 len 123 (local)
Jan 24 20:04:55.510:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.00-00, seq 23E, csum D20D, ht 120,
 len 100 (local)
Jan 24 20:04:56.494:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/0, cnt 0/1, ht 30
Jan 24 20:04:56.502:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.01-00, seq 21C, csum 413, ht 120,
 len 58 (local)
Jan 24 20:04:58.230:ISIS-NSF:Rcv LSP - L2 000C.0000.0000.00-00, seq 11A, csum E197, ht 1194,
 len 88 (Gi2/0/0)
Jan 24 20:05:00.554:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.00-00, seq 23F, csum 1527, ht 120,
 len 111 (local)
```

Related Commands

Command	Description
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interface wait	Specifies how long an 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.

debug mpls traffic-eng ha sso

To display debugging output for Multiprotocol Label Switching (MPLS) traffic engineering high availability (HA) activities during the graceful switchover from an active Route Processor (RP) to a redundant standby RP, use the **debug mpls traffic-eng ha sso** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug mpls traffic-eng ha sso {**auto-tunnel**| **errors**| **link-management** {**events**| **standby**| **recovery**| **checkpoint**}| **tunnel** {**events**| **standby**| **recovery**}}

no debug mpls traffic-eng ha sso {**auto-tunnel**| **errors**| **link-management** {**events**| **standby**| **recovery**| **checkpoint**}| **tunnel** {**events**| **standby**| **recovery**}}

Syntax Description

auto-tunnel	Displays information about autotunnel activity during the MPLS traffic engineering stateful switchover (SSO) process.
errors	Displays errors encountered during the MPLS traffic engineering SSO process.
link-management	Displays information about link management activity during the MPLS traffic engineering SSO process.
events	Displays significant events that occur during the MPLS traffic engineering SSO process.
standby	Displays information about the standby behavior during the MPLS traffic engineering SSO process.
recovery	Displays information about recovery activity during the MPLS traffic engineering SSO process.
checkpoint	Display information about checkpointing activities during the MPLS traffic engineering SSO process. Checkpointing occurs when a message is sent and acknowledged.
tunnel	Displays information about tunnel activity during the MPLS traffic engineering SSO process.

Command Default

Debugging is disabled until you issue this command with one or more keywords.

Command Modes

Privileged EXEC (#)

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays debugging output about the SSO process for MPLS traffic engineering tunnels, autotunnels, and link management systems. The SSO process occurs when the active router becomes unavailable and system control and routing protocol execution is transferred from the now inactive RP to the redundant standby RP, thus providing uninterrupted network services.

Examples

The following is sample output from the **debug mpls traffic-eng ha sso** command when you enabled debugging keywords to monitor the SSO process for tunnels and link management systems as the standby router becomes active:

```
Router# debug mpls traffic-eng ha sso link-management events
MPLS traffic-eng SSO link management events debugging is on
Router# debug mpls traffic-eng ha sso link-management recovery
MPLS traffic-eng SSO link management recovery debugging is on
Router# debug mpls traffic-eng ha sso link-management standby
MPLS traffic-eng SSO link management standby behavior debugging is on
Router# debug mpls traffic-eng ha sso link-management
checkpoint
MPLS traffic-eng SSO link management checkpointed info debugging is on
Router# debug mpls traffic-eng ha sso tunnel standby
MPLS traffic-eng SSO tunnel standby behavior debugging is on
Router# debug mpls traffic-eng ha sso tunnel recovery
MPLS traffic-eng SSO tunnel head recovery debugging is on
Router# debug mpls traffic-eng ha sso tunnel events
MPLS traffic-eng SSO events for tunnel heads debugging is on
Router# debug mpls traffic-eng ha sso errors
MPLS traffic-eng SSO errors debugging is on
Router# show debug
<-----
This command displays the debugging that is enabled.
MPLS TE:
  MPLS traffic-eng SSO link management events debugging is on
  MPLS traffic-eng SSO link management recovery debugging is on
  MPLS traffic-eng SSO link management standby behavior debugging is on
  MPLS traffic-eng SSO link management checkpointed info debugging is on
  MPLS traffic-eng SSO tunnel standby behavior debugging is on
  MPLS traffic-eng SSO tunnel head recovery debugging is on
  MPLS traffic-eng SSO events for tunnel heads debugging is on
  MPLS traffic-eng SSO errors debugging is on
Router#
Standby-Router#
```

Following is the sample debugging output displayed during a successful SSO recovery on the standby router as it becomes active:

```
*May 12 20:03:15.303: RRR_HA_STATE: Told to wait for IGP convergence
*May 12 20:03:14.807: %FABRIC-SP-STDBY-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in
```

```
 slot 5 became active.
*May 12 20:03:15.763: RRR_HA_REC: Attempting to recover last flooded info; protocol: OSPF,
 area: 0
*May 12 20:03:15.763: RRR_HA_REC: recovered ospf area 0 instance 0x48FFF240
*May 12 20:03:15.763: RRR_HA_REC: recovered system info
*May 12 20:03:15.763: RRR_HA_REC: recovered link[0] info
*May 12 20:03:15.763: RRR_HA: Recovered last flooded info for igp: OSPF, area: 0
*May 12 20:03:15.763: Pre announce tunnel 10
*May 12 20:03:15.763: TSPVIF_HA_EVENT: added Router_t10 to dest list
*May 12 20:03:15.763: TSPVIF_HA_EVENT: Completed announcement of 1 tunnel heads to IGP
*May 12 20:03:15.763: TSPVIF_HA_REC: Attempting to recover Tunnel10 after SSO
*May 12 20:03:15.763: LSP-TUNNEL-REOPT: Tunnel10 [61] set to recover
*May 12 20:03:15.763: TSPVIF_HA_REC: Recovered number hops = 5
*May 12 20:03:15.763: TSPVIF_HA_REC: recovered ospf area 0 instance 0x48FFF240
*May 12 20:03:15.763: TSPVIF_HA_REC: Recovered Hop 0: 10.0.3.1, Id: 10.0.0.3 Router Node
(ospf) flag:0x0
*May 12 20:03:15.763: TSPVIF_HA_REC: Recovered Hop 1: 10.0.3.2, Id: 10.0.0.7 Router Node
(ospf) flag:0x0
*May 12 20:03:15.763: TSPVIF_HA_REC: Recovered Hop 2: 10.0.6.1, Id: 10.0.0.7 Router Node
(ospf) flag:0x0
*May 12 20:03:15.763: TSPVIF_HA_REC: Recovered Hop 3: 10.0.6.2, Id: 10.0.0.9 Router Node
(ospf) flag:0x0
*May 12 20:03:15.763: TSPVIF_HA_REC: Recovered Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node
(ospf) flag:0x0
*May 12 20:03:15.763: TSPVIF_HA_REC: signalling recovered setup for Tunnel10: popt 1
[61], weight 2
*May 12 20:03:15.891: TSPVIF_HA_REC: recovered Tu10 forwarding info needed by query
*May 12 20:03:15.891: TSPVIF_HA_REC:     output_idb: GigabitEthernet3/2, output_nhop:
180.0.3.2
Standby-Router#
Router#
*May 12 20:03:25.891: TSPVIF_HA_REC: recovered Tu10 forwarding info needed by query
*May 12 20:03:25.891: TSPVIF_HA_REC:     output_idb: GigabitEthernet3/2, output_nhop:
10.0.3.2
*May 12 20:03:35.891: TSPVIF_HA_REC: recovered Tu10 forwarding info needed by query
*May 12 20:03:35.891: TSPVIF_HA_REC:     output_idb: GigabitEthernet3/2, output_nhop:
10.0.3.2
*May 12 20:03:35.895: RRR_HA_STATE: IGP flood prevented during IGP recovery
*May 12 20:03:38.079: LSP-TUNNEL-REOPT: Tunnel10 [61] received RESV for recovered setup
*May 12 20:03:38.079: LSP-TUNNEL-REOPT: Tunnel10 [61] removed as recovery
*May 12 20:03:38.079: TSPVIF_HA_EVENT: notifying RSVP HA to add lsp_info using key
10.0.0.3->10.0.0.9 Tu10 [61] 10.0.0.3
*May 12 20:03:38.079: TSPVIF_HA_EVENT: updated 7600-1_t10 state; action = add; result =
success
*May 12 20:03:38.079: TSPVIF_HA_EVENT: 7600-1_t10 fully recovered; rewrite refreshed
*May 12 20:03:38.079: TSPVIF_HA_EVENT: notifying CBTS bundle about Router_t10
*May 12 20:03:38.079: TSPVIF_HA_EVENT: notifying RSVP HA to remove lsp_info using key
10.0.0.3->10.0.0.9 Tu10 [61] 10.0.0.3
*May 12 20:03:38.079: RRR_HA: Received notification recovery has ended.  Notify IGP to
flood.
*May 12 20:03:38.079: TSPVIF_HA_EVENT: Received notification recovery has ended
*May 12 20:03:38.079: TSPVIF_HA_STANDBY: prevent verifying setups; IGP has not converged
*May 12 20:03:38.083: TSPVIF_HA_STANDBY: preventing new setups; reason: IGP recovering
*May 12 20:03:38.083: TSPVIF_HA_STANDBY: prevent verifying setups; IGP has not converged
*May 12 20:03:38.083: TSPVIF_HA_STANDBY: preventing new setups; reason: IGP recovering
*May 12 20:03:38.083: RRR_HA_STATE: IGP flood prevented during IGP recovery
7600-1#
*May 12 20:03:47.723: RRR_HA: Received notification that RIB table 0 has converged.
*May 12 20:03:47.723: RRR_HA: Received notification all RIBs have converged.  Notify IGP
to flood.
*May 12 20:03:47.723: RRR_HA_STATE: Told not to wait for IGP convergence
*May 12 20:03:47.723: RRR_HA_INFO: update flooded system info; action = add; result = success
*May 12 20:03:47.723: LM System key::
*May 12 20:03:47.723:   Flooding Protocol: ospf
*May 12 20:03:47.723:   IGP Area ID: 0
*May 12 20:03:47.723: LM Flood Data::
*May 12 20:03:47.723:   LSA Valid flags: 0x0  Node LSA flag: 0x0
*May 12 20:03:47.723:   IGP System ID: 10.0.0.3  MPLS TE Router ID: 10.0.0.3
*May 12 20:03:47.723:   Flooded links: 1  TLV length: 0 (bytes)
*May 12 20:03:47.723:   Fragment id: 0
*May 12 20:03:47.723: rrr_ha_lm_get_link_info_size: link size: 212 bytes; num TLVs: 0
*May 12 20:03:47.723: rrr_ha_sizeof_lm_link_info: link size: 212 bytes; num TLVs: 0
*May 12 20:03:47.723: RRR_HA_INFO: update flooded link[0] info; action = add;
```

```
result = success
*May 12 20:03:47.723: RRR HA Checkpoint Info Buffer::
*May 12 20:03:47.723:   Info Handle:          0x490BB1C8
*May 12 20:03:47.723:   Max Size:             212
*May 12 20:03:47.723:   Info Size:            212
*May 12 20:03:47.723:   Info Write Pointer:   0x490BB29C
*May 12 20:03:47.723: LM Link key::
*May 12 20:03:47.723:   Flooding Protocol: ospf  IGP Area ID: 0  Link ID: 0
(GigabitEthernet3/2)
*May 12 20:03:47.723:     Ifnumber: 5  Link Valid Flags: 0x193B
*May 12 20:03:47.723      Link Subnet Type: Broadcast
*May 12 20:03:47.723:     Local Intfc ID: 0  Neighbor Intf ID: 0
*May 12 20:03:47.723:     Link IP Address: 10.0.3.1
*May 12 20:03:47.723:     Neighbor IGP System ID: 10.0.3.2  Neighbor IP Address: 10.0.0.0
*May 12 20:03:47.723:     IGP Metric: 1  TE Metric: 1
*May 12 20:03:47.723:     Physical Bandwidth: 1000000 kbits/sec
*May 12 20:03:47.723:     Res. Global BW: 3000 kbits/sec
*May 12 20:03:47.723:     Res. Sub BW: 0 kbits/sec
*May 12 20:03:47.723:     Upstream::
Router#
*May 12 20:03:47.723:                                 Global Pool   Sub Pool
*May 12 20:03:47.723:                                 -----------   ----------
*May 12 20:03:47.723:     Reservable Bandwidth[0]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[1]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[2]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[3]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[4]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[5]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[6]:            0            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[7]:            0            0 kbits/sec
*May 12 20:03:47.723:     Downstream::
*May 12 20:03:47.723:                                 Global Pool   Sub Pool
*May 12 20:03:47.723:                                 -----------   ----------
*May 12 20:03:47.723:     Reservable Bandwidth[0]:         3000            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[1]:         3000            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[2]:         3000            0 kbits/sec
*May 12 20:03:47.723:     Reservable Bandwidth[3]:         3000            0 kbits/sec
*May 12 20:03:47.727:     Reservable Bandwidth[4]:         3000            0 kbits/sec
*May 12 20:03:47.727:     Reservable Bandwidth[5]:         3000            0 kbits/sec
*May 12 20:03:47.727:     Reservable Bandwidth[6]:         3000            0 kbits/sec
*May 12 20:03:47.727:     Reservable Bandwidth[7]:         2900            0 kbits/sec
*May 12 20:03:47.727:     Affinity Bits: 0x0
*May 12 20:03:47.727:     Protection Type: Capability 0,  Working Priority 0
*May 12 20:03:47.727:     Number of TLVs: 0
*May 12 20:03:47.727: RRR_HA: Updated flood state for ospf area 0 with 1 links); result =
success
Router#
```

The following example shows how to turn off debugging:

```
Router# no debug mpls traffic-eng ha sso link-management events
MPLS traffic-eng SSO link management events debugging is off
Router# no debug mpls traffic-eng ha sso link-management recovery
MPLS traffic-eng SSO link management recovery debugging is off
Router# no debug mpls traffic-eng ha sso link-management standby
MPLS traffic-eng SSO link management standby behavior debugging is off
Router# no debug mpls traffic-eng ha sso link-management checkpoint
MPLS traffic-eng SSO link management checkpointed info debugging is off
Router# no debug mpls traffic-eng ha sso tunnel standby
MPLS traffic-eng SSO tunnel standby behavior debugging is off
Router# no debug mpls traffic-eng ha sso tunnel recovery
MPLS traffic-eng SSO tunnel head recovery debugging is off
Router# no debug mpls traffic-eng ha sso tunnel events
MPLS traffic-eng SSO events for tunnel heads debugging is off
Router# no debug mpls traffic-eng ha errors
MPLS traffic-eng SSO errors debugging is off
```

Related Commands

Command	Description
debug ip rsvp high-availability	Displays debugging output for RSVP HA activities that improve the accessibility of network resources.
debug ip rsvp sso	Displays debugging output for RSVP activities during the graceful switchover from an active RP to a redundant RP.

destination (call home)

To configure the message destination parameters in a profile for Call Home, use the **destination (call home)** command in call home profile configuration mode. To remove the destination parameters, use the **no** form of this command.

destination {**address** {**email** *address*| **http** *url*}| **message-size-limit** *size*| **preferred-msg-format** {**long-text**| **short-text**| **xml**}| **transport-method** {**email**| **http**}}

no destination {**address** {**email** *address*| **http** *url*}| **message-size-limit** *size*| **preferred-msg-format** {**long-text**| **short-text**| **xml**}| **transport-method** {**email**| **http**}}

Syntax Description

address {**email** *address* | **http** *url*	Configures the address type and location to which Call Home messages are sent, where: • **email** *address* --Email address, up to 200 characters. • **http***url* --URL, up to 200 characters.
message-size-limit *size*	Displays maximum Call Home message size for this profile, in bytes. The range is from 50 to 3145728. The default is 3145728.
preferred-msg-format {**long-text** | **short-text** | **xml**}	Specifies the message format for this profile, where: • **long-text**--Format for use in standard e-mail providing a complete set of information in message. • **short-text**--Format for use with text pagers providing a smaller set of information in the message, including host name, timestamp, error message trigger, and severity level. • **xml**--Format that includes a complete set of information in the message, including XML tags. This is the default.
transport-method	Specifies the transport method for this profile, where: • **email**--Messages are sent using e-mail. This is the default. • **http**--Messages are sent using HTTP or HTTPS.

Command Default

No destination address type is configured. If you do not configure the **destination (call home)** command, the following defaults are configured for the profile:

- **message-size-limit**--3,145,728 bytes
- **preferred-msg-format**--XML
- **transport-method**--E-mail

Command Modes

Call home profile configuration (cfg-call-home-profile)

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

You can repeat the **destination (call home)** command in call home profile configuration mode to configure different message parameters for a profile. There is no default for the **destination address** form of the command, and an address must be configured for every profile.

For a user-defined profile, you can enable both e-mail and HTTP as accepted transport methods, by entering the **destination transport-method email** command and also the **destination transport-method http** command for the profile.

For the CiscoTAC-1 predefined profile, only one transport method can be enabled at a time. If you enable a second transport method, the existing method is automatically disabled. By default, e-mail can be used to send information to the Cisco Smart Call Home backend server, but if you want to use a secure HTTPS transport, you need to configure HTTP.

Examples

The following examples shows configuration of both transport methods for a user profile:

```
Router(config)# call-home
Router(cfg-call-home)# profile example
Router(cfg-call-home-profile)# destination transport-method email
Router(cfg-call-home-profile)# destination transport-method http
```

The following example shows a profile configuration for e-mail messaging using long-text format:

```
Router(config)# call-home
Router(cfg-call-home)# profile example
Router(cfg-call-home-profile)# destination address email username@example.com
Router(cfg-call-home-profile)# destination preferred-msg-format long-text
```

The following example shows part of a Syslog alert notification (when subscribed to receive syslog alerts) using long-text format on a Cisco ASR 1006 router:

```
TimeStamp : 2009-12-03 12:26 GMT+05:00
Message Name : syslog
Message Type : Call Home
Message Group : reactive
Severity Level : 2
Source ID : ASR1000
Device ID : ASR1006@C@FOX105101DH
Customer ID : username@example.com
Contract ID : 123456789
Site ID : example.com
Server ID : ASR1006@C@FOX105101DH
Event Description : *Dec  3 12:26:02.319 IST: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console
System Name : mcp-6ru-3
Contact Email : username@example.com
Contact Phone : +12223334444
Street Address : 1234 Any Street Any City Any State 12345
Affected Chassis : ASR1006
Affected Chassis Serial Number : FOX105101DH
Affected Chassis Part No : 68-2584-05
Affected Chassis Hardware Version : 2.1
Command Output Name : show logging
Attachment Type : command output
MIME Type : text/plain
Command Output Text :
Syslog logging: enabled (1 messages dropped, 29 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 112 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level informational, 104 message lines logged
Log Buffer (1000000 bytes):
*Dec  3 07:16:55.020: ASR1000-RP HA: RF status CID 1340, seq 93, status
RF_STATUS_REDUNDANCY_MODE_CHANGE, op 0, state DISABLED, peer DISABLED
*Dec  3 07:17:00.379: %ASR1000_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-intf
created with ID 4085, ipv4 table-id 0xFF5, ipv6 table-id 0x1E000001
*Dec  3 07:17:00.398: %NETCLK-5-NETCLK_MODE_CHANGE: Network clock source not available. The
 network clock has changed to freerun
*Dec  3 07:17:00.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state
 to up
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down
*Dec  3 07:17:01.818: %DYNCMD-7-CMDSET_LOADED: The Dynamic Command set has been loaded from
```

```
 the Shell Manager
*Dec  3 07:16:30.926: %CMRP-5-PRERELEASE_HARDWARE: R0/0: cmand:  2 is pre-release hardware
*Dec  3 07:16:24.147: %HW_IDPROM_ENVMON-3-HW_IDPROM_CHECKSUM_INVALID: F1: cman_fp:  The
idprom contains an invalid checksum in a sensor entry. Expected: 63, calculated: fe
*Dec  3 07:16:24.176: %CMFP-3-IDPROM_SENSOR: F1: cman_fp:  One or more sensor fields from
the idprom failed to parse properly because Success.
*Dec  3 07:16:27.669: %CPPHA-7-START: F1: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:27.839: %CPPHA-7-START: F1: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.659: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.799: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.557: %CPPHA-7-START: F1: cpp_ha:  CPP 0 running init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.812: %CPPHA-7-READY: F1: cpp_ha:  CPP 0 loading and initialization complete
*Dec  3 07:16:33.532: %CPPHA-7-START: F0: cpp_ha:  CPP 0 running init image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:33.786: %CPPHA-7-READY: F0: cpp_ha:  CPP 0 loading and initialization complete
.
.
.
```

Examples

The following example shows part of a Syslog alert notification using XML format on a Cisco ASR 1006 router when the **destination preferred-msg-format xml** command for a profile is configured:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M0:FOX105101DH:CEC1E73E</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2009-12-03 12:29:02 GMT+05:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>ASR1000</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G1:FOX105101DH:CEC1E73E</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2009-12-03 12:29:01 GMT+05:00</ch:EventTime>
<ch:MessageDescription>*Dec  3 12:29:01.017 IST: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>ASR1000 Series Routers</ch:Series>
</ch:Event>
```

```
<ch:CustomerData>
<ch:UserData>
<ch:Email>username@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>username@example.com</ch:CustomerId>
<ch:SiteId>example.com</ch:SiteId>
<ch:ContractId>123456789</ch:ContractId>
<ch:DeviceId>ASR1006@C@FOX105101DH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>mcp-6ru-3</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>username@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+12223334444</ch:ContactPhoneNumber>
<ch:StreetAddress>1234 Any Street Any City Any State 12345</ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>ASR1006</rme:Model>
<rme:HardwareVersion>2.1</rme:HardwareVersion>
<rme:SerialNumber>FOX105101DH</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="68-2584-05" />
<rme:AD name="SoftwareVersion" value="" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.925" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version 12.2(20091118:075558)
[v122_33_xnf_asr_rls6_throttle-mcp_dev_rls6 102]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 18-Nov-09 01:14 by " />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (1 messages dropped, 29 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 114 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level informational, 106 message lines logged
Log Buffer (1000000 bytes):
*Dec  3 07:16:55.020: ASR1000-RP HA: RF status CID 1340, seq 93, status
RF_STATUS_REDUNDANCY_MODE_CHANGE, op 0, state DISABLED, peer DISABLED
*Dec  3 07:17:00.379: %ASR1000_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-intf
created with ID 4085, ipv4 table-id 0xFF5, ipv6 table-id 0x1E000001
*Dec  3 07:17:00.398: %NETCLK-5-NETCLK_MODE_CHANGE: Network clock source not available. The
 network clock has changed to freerun
*Dec  3 07:17:00.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state
 to up
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state
```

```
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down
*Dec  3 07:17:01.818: %DYNCMD-7-CMDSET_LOADED: The Dynamic Command set has been loaded from
 the Shell Manager
*Dec  3 07:16:30.926: %CMRP-5-PRERELEASE_HARDWARE: R0/0: cmand:  2 is pre-release hardware
*Dec  3 07:16:24.147: %HW_IDPROM_ENVMON-3-HW_IDPROM_CHECKSUM_INVALID: F1: cman_fp:  The
idprom contains an invalid checksum in a sensor entry. Expected: 63, calculated: fe
*Dec  3 07:16:24.176: %CMFP-3-IDPROM_SENSOR: F1: cman_fp:  One or more sensor fields from
the idprom failed to parse properly because Success.
*Dec  3 07:16:27.669: %CPPHA-7-START: F1: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:27.839: %CPPHA-7-START: F1: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.659: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.799: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.557: %CPPHA-7-START: F1: cpp_ha:  CPP 0 running init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.812: %CPPHA-7-READY: F1: cpp_ha:  CPP 0 loading and initialization complete
.
.
.
```

Related Commands

Command	Description
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.

issu changeversion

To perform a single-step complete In-Service Software Upgrade (ISSU) upgrade process cycle, use the **issu changeversion** command in privileged EXEC mode.

issu changeversion active-image

Syntax Description

active-image	The active image on the networking device.

Command Default

No upgrade has happened.

Command Modes

Privileged EXEC (#)

Release	Modification
12.2(33)SCD2	This command was introduced.

Usage Guidelines

The **issu changeversion** command starts a single-step complete upgrade process cycle. This command performs the logic for all four of the standard commands (**issu loadversion**, **issu runversion**, **issu acceptversion**, and **issu commitversion**) without any user intervention required to complete the next step.

The **issu changeversion** command allows the networking device to inform the system that the networking device is performing a complete upgrade cycle automatically, and allows the state transitions to move to the next step automatically.

Once the **issu changeversion** command is issued, the upgrade can be aborted using the **issu abortversion** command. An upgrade using the **issu changeversion** command may also be automatically aborted if the system detects any problems or an unhealthy system is determined during the upgrade.

The ISSU upgrade process consists of three states:

1. Initialization (INIT) state
2. Load version (LV) state
3. Run version (RV) state

Each of these states is defined by a set of variables, which are primary version (PV), secondary version (SV), current version (CV), and the ISSU state (IS). The transition of all these states is accomplished using the **issu changeversion** command, which automatically performs these state transitions.

Examples

The following example starts a single-step complete upgrade process cycle using the disk0:ubr10k4-k9p6u2-mz.122-33.SCC2 image from slot 0:

```
Router# issu changeversion
disk0:ubr10k4-k9p6u2-mz.122-33.SCC2
```

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 commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover from the active RP to the standby RP and causes the newly active RP to run the new image specified in the **issu loadversion** command.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu commitversion

To allow the new Cisco IOS software image to be loaded into the standby Route Processor (RP), use the **issu commitversion** command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 Series Routers.

General Syntax

issu commitversion *slot active-image*

Cisco ASR 1000 Series Routers Syntax

issu commitversion [verbose]

Syntax Description

slot	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
active-image	The new image to be loaded into the active networking device.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

This command is disabled by default.

Command Modes

User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. In Service Software Upgrade (ISSU) is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the ASR 1000 Series Routers, and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **issu commitversion** command verifies that the standby RP has the new Cisco IOS software image in its file system and that both RPs are in the run version (RV) state. If these conditions are met, then the following actions take place:

- The standby RP is reset and booted with the new version of Cisco IOS software.
- If both images are compatible, the standby RP moves into the stateful switchover (SSO) mode and is fully stateful for all clients and applications with which the standby RP is compatible.
- If both images are not compatible, the standby RP moves into Route Processor Redundancy Plus (RPR+) mode or RPR mode.
- If all conditions are correct, the RPs are moved into final state, which is the same as initial state.

Issuing the issu commitversion command completes the In Service Software Upgrade (ISSU) process. This process cannot be stopped or reverted to its original state without starting a new ISSU process.

Issuing the **issu commitversion** command at this stage is equivalent to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for a period of time and are satisfied with the new software version.

On Cisco ASR 1000 series routers, the **issu** command set, including this command, can be used to upgrade individual subpackages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

The **issu runversion** step can be bypassed on a Cisco ASR 1000 Series Router by using the **redundancy force-switchover** command to switchover between RPs and entering the **issu commitversion** command on the RP being upgraded. However, the **issu runversion** command is still available on this router and can still be used as part of the process for upgrading software using ISSU.

Previously, when ISSU was in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run was not present, the only way to return to the ISSU Init state was to clear the state manually and reload the router. Now, if either the i**ssu commitversion** or the **issu runversion** command is issued and the image cannot be located, the ISSU state is cleared automatically, and the standby RP is reloaded with the image that existed before the i**ssu abortversion** or the **issu loadversion** command was issued.

Examples

The following example shows how to reset the standby RP and reload it with the new Cisco IOS software version:

```
Router# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830
```

The following example shows how the standby RP or Cisco IOS process is reset and reloaded with the new Cisco consolidated package on the Cisco ASR 1000 Series Router:

```
Router# issu commitversion
--- Starting installation changes ---
Cancelling rollback timer
Saving image changes
Finished installation changes
Building configuration...
[OK]
SUCCESS: version committed: harddisk
:ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin
```

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.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu loadversion

To start the In Service Software Upgrade (ISSU) process, use the **issu loadversion** command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 series routers.

General Syntax

issu loadversion *active-slot active-image standby-slot standby-image* **[force]**

Cisco ASR 1000 Series Routers Syntax

issu loadversion rp [**0**| **1**] **file** *file-URL* [**bay** *bay-number*] [**slot** *slot-number*] **[force] [verbose]**

Syntax Description

active-slot	The active slot on the networking device.
active-image	The active image on the networking device.
rp [**0** | **1**]	Specifies the Route Processor (RP) on the Aggregation Services Router to install the Cisco IOS-XE image. Entering **rp 0** selects the RP in slot 0, and entering **rp 1** selects the RP in slot 1.
file*file-URL*	Specifies the URL to the Cisco IOS-XE image file that will be used to perform this upgrade.
standby-slot	The standby slot on the networking device.
standby-image	The new image to be loaded into the standby networking device.
bay bay-number	Specifies the bay number within a SIP where a SPA is installed.
slot slot-number	Specifies the router slot number where a SIP is installed.
force	(Optional) Used to override the automatic rollback when the new Cisco IOS software version is detected to be incompatible, which is the case when as user intends to perform a fast software upgrade (FSU) in Route Processor Redundancy (RPR) mode.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default This command is disabled by default.

Command Modes User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. ISSU is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines Enabling the issue loadversion command causes the standby RP to be reset and booted with the new Cisco IOS software image specified by the command. If both the active and standby RP images are ISSU-capable, ISSU-compatible, and have no configuration mismatches, then the standby RP moves into stateful switchover (SSO) mode, and both RPs move into the load version (LV) state.

It may take several seconds after the **issu loadversion** command is entered for Cisco IOS software to load into the standby RP and the standby RP to transition to SSO mode.

Cisco ASR 1000 Series Routers Usage Guidelines

On Cisco ASR 1000 Series Routers, the **issu** command set, including this command, can be used to upgrade individual sub-packages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

The ISSU rollback timer starts at **issu loadversion** on the Cisco ASR 1000 Series Routers.

Previously, when ISSU was in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run was not present, the only way to return to the ISSU Init state was to clear the state manually and reload the router. Now, if either the i**ssu commitversion** or the **issu runversion** command is issued and the image cannot be located, the ISSU state is cleared

automatically, and the standby RP is reloaded with the image that existed before the i**ssu abortversion** or the **issu loadversion** command was issued.

Examples

The following example shows how to initiate the ISSU process by loading the active image into the active RP slot and loading the standby image into the standby RP slot:

```
Router# issu loadversion a disk0:c10k2-p11-mz.2.20040830 b stby-disk0:c10k2-p11-mz.2.20040830
```

The following example shows how to initiate an ISSU consolidated package upgrade on a Cisco ASR 1000 Series Router.

```
Router# issu loadversion rp 1 file
stby-harddisk:ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin
--- Starting installation state synchronization --- Finished installation state
synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting system installation readiness checking --- Finished system installation readiness
 checking
--- Starting installation changes ---
Setting up image to boot on next reset
Starting automatic rollback timer
Finished installation changes
SUCCESS: Software will now load.
```

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 commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu runversion

To force a switchover from the active Route Processor (RP) to the standby RP and cause the newly active RP to run the new image specified in the **issu loadversion** command, use the **issu runversion** command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 Series Routers.

General Syntax

issu runversion *slot image*

Cisco ASR 1000 Series Routers Syntax

issu runversion [verbose]

Syntax Description

slot	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
image	The new image to be loaded into the standby RP.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

No default behavior or values.

Command Modes

User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. ISSU is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

When a user enables the **issu runversion** command, a switchover is performed, and the standby RP is booted with the old image version following the reset caused by the switchover. As soon as the standby RP moves into the standby state, the rollback timer is started.

On Cisco ASR 1000 Series Routers, the **issu** command set, including this command, can be used to upgrade individual sub-packages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

The **issu runversion** step can be bypassed on a Cisco ASR 1000 Series Router by using the **redundancy force-switchover** command to switchover between RPs and entering the **issu commitversion** command on the RP being upgraded. However, **issu runversion** is still available on this router and can still be used as part of the process for upgrading software using ISSU.

Previously, when ISSU was in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run was not present, the only way to return to the ISSU Init state was to clear the state manually and reload the router. Now, if either the i**ssu commitversion** or the **issu runversion** command is issued and the image cannot be located, the ISSU state is cleared automatically, and the standby RP is reloaded with the image that existed before the i**ssu abortversion** or the **issu loadversion** command was issued.

Examples

In the following example, the **issu runversion** command is used to switch to the redundant RP with the new Cisco IOS software image:

```
Router# issu runversion b stby-disk0:c10k2-p11-mz.2.20040830
```

In the following example, the **issu runversion** command is used to switch to the standby RP with the new Cisco IOS-XE consolidated package on the Cisco ASR 1000 Series Routers:

```
Router# issu runversion
--- Starting installation state synchronization ---
Finished installation state synchronization
Initiating active RP failover
SUCCESS: Standby RP will now become active
```

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.

Command	Description
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Commits the new Cisco IOS software image in the file system of the standby RP and ensures that both the active and standby RPs are in the RV state.
issu loadversion	Starts the ISSU process.
show issu state	Displays the state and current version of the RPs during the ISSU process.

M through Service

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-address*| *name*} **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)

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

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.

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.

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)

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

Release	Modification
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.

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.

Command	Description
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.

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* **ha-mode sso**

no neighbor *ip-address* **ha-mode sso**

Syntax Description

ip-address	IP address of the neighboring router.

Command Default

BGP NSR with SSO support is disabled.

Command Modes

Address family configuration Session-template configuration

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.

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 IPv4 VRF 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 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 Enhanced Interior Gateway Protocol (EIGRP), use the **nsf** command in router configuration mode or address-family configuration mode. To disable EIGRP NSF and remove the EIGRP NSF configuration from the running-config file, use the **no** form of this command.

nsf

no nsf

Syntax Description

This command has no arguments or keywords.

Command Default

EIGRP NSF capability is enabled by default.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af)

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. Address-family configuration mode was added.
12.2(33)SRE	This command was modified. 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.

Usage Guidelines

This command is used to enable or disable EIGRP NSF support on an NSF capable router. EIGRP NSF capability is enabled by default on distributed platforms that run a supporting version of Cisco IOS software.

Examples

The nsf command is used to enable or disable the EIGRP NSF capability. The following example disables NSF capability:

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# no nsf
```

The nsf command is used to enable or disable the EIGRP NSF capability. The following EIGRP named configuration example disables NSF capability:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 as 10
Router(config-router-af)# no nsf
```

Related Commands

Command	Description
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. This output includes NSF notifications and events.
show ip protocols	Displays the parameters and current state of the active routing protocol process. The status of EIGRP NSF configuration and support is displayed in the output.
timers nsf converge	Adjusts the maximum time that restarting router will wait for the EOT notification from an NSF-capable or NSF-aware peer.
timers nsf route-hold	Adjusts the maximum period of time that a supporting peer will hold known routes for an NSF-capable router during a restart operation or during a well-known failure condition.
timers nsf signal	Adjusts the maximum time for the initial restart period.

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)

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 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)

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 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

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.

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.

profile *profile-name*

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

Syntax Description

profile-name	Name of the destination profile.
all	Removes all user-defined destination profiles.

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)

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.

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)

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.

Release	Modification
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.
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
```

Examples

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
```

Examples

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

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

Examples

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.
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.

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf commandrouter ospf *process-id* [**vrf** *vpn-name*]

no router ospf *process-id* [**vrf** *vpn-name*]

Syntax Description

process-id	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
vrf *vpn-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.

Command Default

No OSPF routing process is defined.

Command Modes

Global configuration

Release	Modification
10.0	This command was introduced.
12.0(7)T	The **vrf** keyword and *vpn-name* arguments were added to identify a VPN.
12.0(9)ST	The **vrf** keyword and *vpn-name* arguments were 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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify multiple OSPF routing processes in each router.

After you enter the **router ospf** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

Examples

The following example configures an OSPF routing process and assign a process number of 109:

```
Router(config)# router ospf 109
```

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF instance processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12 vrf first
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)# exit
```

The following example shows usage of the **maximum-paths** option:

```
Router> enable
Router# configure terminal
Router(config)# router ospf

Router(config-router)# maximum-paths?
Router(config-router)# 20

Router(config-router)# exit
```

Related Commands

Command	Description
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

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)

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.

Command	Description
call-home test	Manually sends a Call Home test message to a destination profile.
show call-home	Displays Call Home configuration information.

Show through Z

show call-home

To display the configured information for Call Home, use the **show call-home** command in privileged EXEC mode.

show call-home [**alert-group**| **detail**| **mail-server status**| **profile** {**all**| *name*}| **statistics**]

Syntax Description

alert-group	(Optional) Displays the available alert groups.
detail	(Optional) Displays the Call Home configuration in detail.
mail-server status	(Optional) Displays mail-server status information for Call Home.
profile {**all** | *name*	(Optional) Displays configuration information for Call Home destination profiles, where: • **all**--Displays information for all configured profiles. • *name*--Name of a specific profile about which to display information.
statistics	(Optional) Displays Call Home statistics.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

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 displays the Call Home configuration settings:

```
Router# show call-home
Current call home settings:
    call home feature : disable
    call home message's from address: switch@example.com
    call home message's reply-to address: support@example.com
    contact person's email address: technical@example.com
    contact person's phone number: +1-111-111-1111
    street address: 1234 Any Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    Rate-limit: 20 message(s) per minute
Available alert groups:
    Keyword                 State   Description
    ----------------------- ------- --------------------------------
    configuration           Disable configuration info
    diagnostic              Disable diagnostic info
    environment             Disable environmental info
    inventory               Enable  inventory info
    syslog                  Disable syslog info
Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
```

The following example displays detailed configuration information for Call Home:

```
Router# show call-home detail

Current call home settings:
    call home feature : disable
    call home message's from address: switch@example.com
    call home message's reply-to address: support@example.com
    contact person's email address: technical@example.com
    contact person's phone number: +1-111-111-1111
    street address: 1234 Any Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    Rate-limit: 20 message(s) per minute
Available alert groups:
    Keyword                 State   Description
    ----------------------- ------- --------------------------------
    configuration           Disable configuration info
    diagnostic              Disable diagnostic info
    environment             Disable environmental info
    inventory               Enable  inventory info
    syslog                  Disable syslog info
Profiles:
    Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Preferred Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up
    Alert-group              Severity
    -----------------------  ------------
    inventory                normal
    Syslog-Pattern           Severity
    -----------------------  ------------
    N/A                      N/A
Profile Name: CiscoTAC-1
```

```
    Profile status: INACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Preferred Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): Not yet set up
    Periodic configuration info message is scheduled every 1 day of the month at 09:27
    Periodic inventory info message is scheduled every 1 day of the month at 09:12
    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               minor
    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

The following example displays available Call Home alert groups:

```
Router# show call-home alert-group
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Disable configuration info
    diagnostic               Disable diagnostic info
    environment              Disable environmental info
    inventory                Enable  inventory info
    syslog                   Disable syslog info
```

The following example displays e-mail server status information for Call Home:

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...
Translating "smtp.example.com"
    Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
    Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]
```

The following example displays information for all predefined and user-defined profiles for Call Home:

```
Router# show call-home profile all
Profile Name: campus-noc
Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Preferred Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up
    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A
Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Preferred Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): Not yet set up
    Periodic configuration info message is scheduled every 1 day of the month at 09:27
    Periodic inventory info message is scheduled every 1 day of the month at 09:12
    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               minor
    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

The following example displays information for a user-defined destination profile named “campus-noc”:

```
Router# show call-home profile campus-noc
Profile Name: campus-noc
```

```
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Preferred Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up
    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A
```

The following example displays Call Home statistics:

```
Router# show call-home statistics

Successful Call-Home Events: 0
Dropped Call-Home Events due to Rate Limiting: 0
```

The following example shows a sample of the Call Home statistics output on a Cisco ASR 1000 Series Router in Cisco IOS XE Release 2.6:

```
PE42_ASR-1004#show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total Failed    0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Last call-home message sent time: n/a
```

Related Commands

Command	Description
call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
service call-home	Enables Call Home.

show ip bgp vpnv4 all sso summary

To display information about Border Gateway Protocol (BGP) peers that support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **show ip bgp vpn4 sso summary** command in privileged EXEC mode.

show ip bgp vpnv4 all sso summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

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.

Usage Guidelines

The **show ip bgp vpnv4 all sso summary** command is used to display the number of BGP neighbors that are in SSO mode.

Examples

The following is sample output from the **show ip bgp vpnv4 all sso summary** command:

```
Router# show ip bgp vpnv4 all sso summary
   Stateful switchover support enabled for 40 neighbors
```

Table 1 describes the significant fields shown in the display.

Table 1: show ip bgp vpnv4 all sso summary Field Descriptions

Field	Description
Stateful Switchover support enabled for	Indicates the number of BGP neighbors that are in SSO mode.

Related Commands

Command	Description
neighbor ha-mode sso	Configures a BGP neighbor to support SSO.

show ip ospf nsf

To display IP Open Shortest Path First (OSPF) nonstop forwarding (NSF) state information, use the **show ip ospf nsf** command in user EXEC or privileged EXEC mode.

show ip ospf nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Mainline Release	Modification
12.2(33)SXI	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

The following is sample output from the **show ip ospf nsf** command. The fields are self-explanatory.

```
Router# show ip ospf
 nsf
Routing Process "ospf 2"
 Non-Stop Forwarding enabled
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 OSPF restart state is NO_RESTART
Handle 1786466308, Router ID 192.0.2.1, checkpoint Router ID 0.0.0.0
Config wait timer interval 10, timer not running
Dbase wait timer interval 120, timer not running
```

show ip rsvp high-availability counters

To display all Resource Reservation Protocol (RSVP) traffic engineering (TE) high availability (HA) counters that are being maintained by a Route Processor (RP), use the **show ip rsvp high-availability counters** command in user EXEC or privileged EXEC mode.

show ip rsvp high-availability counters

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SRB	Support for In-Service Software Upgrade (ISSU) was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)S	This command was modified. The output was updated to display information for point-to-point (P2P) and point-to-multipoint traffic engineering (P2MP) counters.

Usage Guidelines

Use the **show ip rsvp high-availability counters** command to display the HA counters, which include state, ISSU, checkpoint messages, resource failures, and errors.

The command output differs depending on whether the RP is active or standby. (See the “Examples” section for more information.)

Use the **clear ip rsvp high-availability counters** command to clear all counters.

Examples

The following is sample output from the **show ip rsvp high-availability counters** command on the active RP:

```
Router# show ip rsvp high-availability counters
State: Active
P2P LSPs for which recovery:
  Attempted: 1
  Succeeded: 1
  Failed:    0
P2MP subLSPs for which recovery:
  Attempted: 2
  Succeeded: 2
  Failed:    0
Bulk sync
```

```
  initiated: 1
Send timer
  started: 2
Checkpoint Messages (Items) Sent
  Succeeded:      2  (8)
    Acks accepted:2  (8)
    Acks ignored:     (0)
    Nacks:        0  (0)
  Failed:         0  (0)
  Buffer alloc:   2
  Buffer freed:   4
ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         2
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         2
      Failed:            0
      Transformations:   0
  Negotiation:
    Started:              2
    Finished:             2
    Failed to Start:      0
    Messages:
      Sent:
        Send succeeded:   14
        Send failed:      0
        Buffer allocated:        14
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        10
        Failed:           0
        Buffer freed:     10
  Init:
    Succeeded:            1
    Failed:               0
  Session Registration:
    Succeeded:            1
    Failed:               0
  Session Unregistration:
    Succeeded:            1
    Failed:               0
Errors:
  None
Historical: (When Active was Standby)
Checkpoint Messages (Items) Received
  Valid:        2  (11)
  Invalid:      0  (0)
Buffer freed: 2
```

Table 1 describes the significant fields shown in the display.

Table 2: show ip rsvp high-availability counters--Active RP Field Descriptions

Field	Description
State	The RP state: • Active--Active RP.
Bulk sync	The number of requests made by the standby RP to the active RP to resend all write database entries: • Initiated--The number of bulk sync operations initiated by the standby RP since reboot.

Field	Description
Send timer	The write database timer.
Checkpoint Messages (Items) Sent	The details of the bundle messages or items sent since booting.
Succeeded	The number of bundle messages or items sent from the active RP to the standby RP since booting. Values are the following: • Acks accepted--The number of bundle messages or items sent from the active RP to the standby RP. • Acks ignored--The number of bundle messages or items sent by the active RP, but rejected by the standby RP. • Nacks--The number of bundle messages or items given to the checkpointing facility (CF) on the active RP for transmitting to the standby RP, but failed to transmit.
Failed	The number of bundle messages or items the active RP attempted to send the standby RP when the send timer updated, but received an error back from CF.
Buffer alloc	Storage space allocated.
Buffer freed	Storage space available.
ISSU	In-Service Software Upgrade (ISSU) counters.
Checkpoint Messages Transformed	The details of the bundle messages or items transformed (upgraded or downgraded for compatibility) since booting so that the active RP and the standby RP can interoperate.
On Send	The number of messages sent by the active RP that succeeded, failed, or were transformations.
On Recv	The number of messages received by the active RP that succeeded, failed, or were transformations.
Negotiation	The number of times that the active RP and the standby RP have negotiated their interoperability parameters.
Started	The number of negotiations started.
Finished	The number of negotiations finished.

Field	Description
Failed to Start	The number of negotiations that failed to start.
Messages	The number of negotiation messages sent and received. These messages can be succeeded or failed. • Send succeeded--Number of messages sent successfully. • Send failed--Number of messages sent unsuccessfully. • Buffer allocated--Storage space allowed. • Buffer freed--Storage space available. • Buffer alloc failed--No storage space available.
Init	The number of times the RSVP ISSU client has successfully and unsuccessfully (failed) initialized.
Session Registration	The number of session registrations, succeeded and failed, performed by the active RP whenever the standby RP reboots.
Session Unregistration	The number of session unregistrations, succeeded and failed, before the standby RP resets.
Errors	The details of errors or caveats.

The following is sample output from the **show ip rsvp high-availability counters** command on the standby RP:

```
Router# show ip rsvp high-availability counters
State: Standby

Checkpoint Messages (Items) Received
  Valid:        1  (2)
  Invalid:      0  (0)
  Buffer freed: 1

ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         0
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         1
      Failed:            0
      Transformations:   0

  Negotiation:
    Started:              1
    Finished:             1
    Failed to Start:      0
    Messages:
      Sent:
```

```
        Send succeeded:   5
        Send failed:      0
        Buffer allocated:        5
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        7
        Failed:           0
        Buffer freed:     7

  Init:
    Succeeded:            1
    Failed:               0

  Session Registration:
    Succeeded:            0
    Failed:               0

  Session Unregistration:
    Succeeded:            0
    Failed:               0

Errors:
  None
```

Table 2 describes the significant fields shown in the display.

Table 3: show ip rsvp high-availability counters--Standby RP Field Descriptions

Field	Description
State	The RP state: • Standby--Standby (backup) RP.
Checkpoint Messages (Items) Received	The details of the messages or items received by the standby RP. Values are the following: • Valid--The number of valid messages or items received by the standby RP. • Invalid--The number of invalid messages or items received by the standby RP. • Buffer freed--Amount of storage space available.
ISSU	ISSU counters. **Note** For descriptions of the ISSU fields, see Table 1 .
Errors	The details of errors or caveats.

Related Commands

Command	Description
clear ip rsvp high-availability counters	Clears (sets to zero) the RSVP-TE HA counters that are being maintained by an RP.

Command	Description
show ip rsvp high-availability database	Displays the contents of the RSVP-TE HA read and write databases used in TE SSO.
show ip rsvp high-availability summary	Displays summary information for an RSVP-TE HA RP.

show isis nsf

To display current state information regarding Intermediate System-to-Intermediate System (IS-IS) Cisco nonstop forwarding (NSF), use the **show isis nsf** command in user EXEC mode.

show isis nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

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 **show isis nsf** command can be used with both Cisco proprietary IS-IS NSF and Internet Engineering Task Force (IETF) IS-IS NSF. The information displayed when this command is entered depends on which protocol has been configured. To configure nsf for a specific routing protocol, use the **router bgp**, **router ospf**, or **router isis** commands in global configuration mode.

Examples

The following example shows state information for an active RP that is configured to use Cisco proprietary IS-IS NSF:

```
Router# show isis nsf
NSF 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
```

Table 1 describes the significant fields shown in the display.

Table 4: show isis nsf Field Descriptions

Field	Description
NSF enabled, mode 'cisco'	NSF is enabled in the default cisco mode.
RP is ACTIVE, standby ready, bulk sync complete	Status of the active RP, standby RP, and the synchronization process between the two.
NSF interval timer expired (NSF restart enabled)	NSF interval timer has expired, allowing NSF restart to be active.
Checkpointing enabled, no errors	Status of the checkpointing process.
Local state:ACTIVE, Peer state:STANDBY HOT, Mode:SSO	State of the local RP, the peer RP, and the operating mode these RPs are using.

The following example shows state information for a standby RP that is configured to use Cisco proprietary IS-IS NSF:

```
Router# show isis nsf
NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 314
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

The following example shows state information when the networking device is configured to use IETF IS-IS NSF:

```
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
```

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 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.
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 ES and IS neighbors.

show issu

To display Enhanced Fast Software Upgrade (eFSU) information, use the **show issu** command.

show issu {**outage slot** {**all**| *num*}| **patch context**| **patch type** *image*| **platform states**}

Syntax Description

outage slotall	Displays an average estimate of the traffic outage for all slots during the upgrade or downgrade.
outage slot*num*	Displays an average estimate of the traffic outage to expect per a specific slot during the upgrade/downgrade.
patch context	Displays the patch context during the patch installation and activation.
patch type *image*	Displays patch information about the image that you are about to upgrade to.
platform states	Displays the state of the platform specific eSFU data.

Command Default

None

Command Modes

User EXEC (>) Privileged EXEC (#)

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Examples

The following example shows how to display an average estimate of the traffic outage for all slots during the upgrade or downgrade:

```
Router# show issu outage slot all

Slot # Card Type                                MDR Mode          Max Outage Time
------ ---------------------------------------  -----------       ---------------
     1 CEF720 24 port 1000mb SFP                WARM_RELOAD        300 secs
     2 1-subslot SPA Interface Processor-600    WARM_RELOAD        300 secs
     3 4-subslot SPA Interface Processor-400    WARM_RELOAD        300 secs
     4 2+4 port GE-WAN                          RELOAD             360 secs
Router#
```

Related Commands

Command	Description
issu	Sets up an Enhanced Fast Software Upgrade (eFSU).

show issu rollback timer

To display the current setting of the In Service Software Upgrade (ISSU) rollback timer, use the **show issu rollback timer** command in user EXEC or privileged EXEC mode.

show issu rollback timer

Syntax Description

This command has no arguments or keywords.

Command Default

The default rollback timer value is 45 minutes.

Command Modes

User EXEC (>) Privileged EXEC (#)

Release	Modification
12.2(28)SB	This command was introduced.
12.2(28)SB2	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7500 series routers.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

If the ISSU rollback timer value has never been set, then the default rollback timer value of 45 minutes is displayed.

Examples

The following example shows the default rollback timer value:

```
Router# show issu rollback-timer
Rollback Process State = Not in progress
Configured Rollback Time = 45:00
```

Table 1 describes the significant fields shown in the display.

Table 5: show issu rollback-timer Field Descriptions

Field	Description
Rollback Process State = Not in progress	State of the rollback process.
Configured Rollback Time = 45:00	Rollback timer value.

Related Commands

Command	Description
configure issu set rollback timer	Configures the rollback timer value.

show redundancy

To display current or historical status and related information on planned or logged handovers, use the **show redundancy** command in user EXEC or privileged EXEC mode.

Privileged EXEC Mode

show redundancy [**clients**| **counters**| **debug-log**| **handover**| **history**| **switchover history**| **states**| **inter-device**]

User EXEC Mode

show redundancy {**clients**| **counters**| **history**| **states**| **switchover**}

Syntax Description

clients	(Optional) Displays the redundancy-aware client-application list.
counters	(Optional) Displays redundancy-related operational measurements.
debug-log	(Optional) Displays up to 256 redundancy-related debug entries.
handover	(Optional) Displays details of any pending scheduled handover.
history	(Optional) Displays past status and related information about logged handovers. This is the only keyword supported on the Cisco AS5800.
switchover history	(Optional) Displays redundancy switchover history.
states	(Optional) Displays redundancy-related states: disabled, initialization, standby, active (various substates for the latter two), client ID and name, length of time since client was sent the progression, and event history for the progression that was sent to the client.
switchover	(Optional) Displays the switchover counts, the uptime since active, and the total system uptime.
inter-device	(Optional) Displays redundancy interdevice operational state and statistics.

Command Modes

User EXEC (>) Privileged EXEC (#)

Release	Modification
11.3(6)AA	This command was introduced in privileged EXEC mode.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5800 and Cisco AS5850 is not included in this release.
12.2(8)MC2	This command was introduced in user EXEC mode.
12.2(11)T	The privileged EXEC mode form of this command was implemented on the Cisco AS5800 and Cisco AS5850.
12.2(14)SX	The user EXEC mode form of this command was introduced on the Supervisor Engine 720.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(20)S	The **states**, **counters**, **clients**, **history**, and **switchover history** keywords were added.
12.2(17d)SXB	Support for the user EXEC mode form of this command was extended to the Supervisor Engine 2.
12.3(8)T	The **inter-device** keyword was added to the privileged EXEC form of the command.
12.3(11)T	The user EXEC form of this command was integrated into Cisco IOS Release 12.3(11)T.
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(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	The clients keyword was enhanced to provide information about the status of each client.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.
12.2(31)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Release	Modification
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	More information regarding the **states** keyword was added.

Usage Guidelines

Cisco AS5800

Use this command from the router-shelf console to determine when failover is enabled. Use this command with the **history** keyword to log failover events.

Cisco AS5850

To use this command, the router must have two route-switch-controller (RSC) cards installed and must be connected to one of them.

Examples

The following example shows how to display information about the RF client:

```
Router# show redundancy clients
 clientID = 0       clientSeq = 0        RF_INTERNAL_MSG
 clientID = 25      clientSeq = 130      CHKPT RF
 clientID = 5026    clientSeq = 130      CHKPT RF
 clientID = 5029    clientSeq = 135      Redundancy Mode RF
 clientID = 5006    clientSeq = 170      RFS client
 clientID = 6       clientSeq = 180      Const OIR Client
 clientID = 7       clientSeq = 190      PF Client
 clientID = 5008    clientSeq = 190      PF Client
 clientID = 28      clientSeq = 330      Const Startup Config
 clientID = 29      clientSeq = 340      Const IDPROM Client
 clientID = 65000   clientSeq = 65000    RF_LAST_CLIENT
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current RF state.

The following example shows how to display information about the RF counters:

```
Router# show redundancy counters
Redundancy Facility OMs
               comm link up = 0
        comm link down down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0
      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
        errored peer msg rx = 0
                 buffers tx = 0
     tx buffers unavailable = 0
                 buffers rx = 0
      buffer release errors = 0
 duplicate client registers = 0
```

```
  failed to register client = 0
       Invalid client syncs = 0
```

The following example shows information about the RF history:

```
Router# show redundancy history
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:02 client added: Const Startup Config Sync Clien(28) seq=330
00:00:02 client added: CHKPT RF(25) seq=130
00:00:02 client added: PF Client(7) seq=190
00:00:02 client added: Const OIR Client(6) seq=180
00:00:02 client added: Const IDPROM Client(29) seq=340
00:00:02 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:02 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) CHKPT RF(25) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) Const OIR Client(6) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) PF Client(7) op=0 rc=11
```

The following example shows information about the RF state:

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 1
Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured)  = Route Processor Redundancy
     Split Mode = Disabled
   Manual Swact = Disabled  Reason: Simplex mode
 Communications = Down      Reason: Simplex mode
   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0
```

If you enter the **show redundancy states** command with stateful switchover (SSO) configured, the Redundancy Mode (Operational) and the Redundancy Mode (Configured) fields display stateful switchover.

The following example shows how to display the switchover counts, the uptime since active, and the total system uptime:

```
Router> show redundancy switchover
Switchovers this system has experienced          : 1
Uptime since this supervisor switched to active  : 1 minute
Total system uptime from reload                  : 2 hours, 47 minutes
```

Examples

The following is sample output from the **show redundancy handover** and **show redundancy states** commands on a Cisco AS5850:

```
Router# show redundancy handover

No busyout period specified
Handover pending at 23:00:00 PDT Wed May 9 2001
Router# show redundancy states

my state = 14 -ACTIVE_EXTRALOAD
peer state = 4 -STANDBY COLD
Mode = Duplex
Unit = Preferred Primary
Unit ID = 6
Redundancy Mode = Handover-split: If one RSC fails, the peer RSC will take over the
feature boards
Maintenance Mode = Disabled
Manual Swact = Disabled Reason: Progression in progress
Communications = Up
```

```
client count = 3
client_notification_TMR = 30000 milliseconds
keep_alive TMR = 4000 milliseconds
keep_alive count = 1
keep_alive threshold = 7
RF debug mask = 0x0
```

Examples The following is sample output from the **show redundancy** command on a Cisco AS5800:

```
Router# show redundancy
DSC in slot 12:
Hub is in 'active' state.
Clock is in 'active' state.
DSC in slot 13:
Hub is in 'backup' state.
Clock is in 'backup' state.
```

Examples The following is sample output from the **show redundancy history** command on a Cisco AS5800:

```
Router# show redundancy history
DSC Redundancy Status Change History:
981130 18:56 Slot 12 DSC: Hub, becoming active - RS instruction
981130 19:03 Slot 12 DSC: Hub, becoming active - D13 order
```

Examples The following is sample output from two Cisco AS5800 router shelves configured as a failover pair. The active router shelf is initially RouterA. The **show redundancy history** and **show redundancy** commands have been issued. The **show redundancy** command shows that failover is enabled, shows the configured group number, and shows that this router shelf is the active one of the pair. Compare this output with that from the backup router shelf (RouterB) that follows.

Note When RouterA is reloaded, thereby forcing a failover, new entries are shown on RouterB when a**show redundancy history** command is issued after failover has occurred.

Examples

```
RouterA# show redundancy history
DSC Redundancy Status Change History:
010215 18:17 Slot -1 DSC:Failover configured -> ACTIVE role by default.
010215 18:18 Slot -1 DSC:Failover -> BACKUP role.
010215 18:18 Slot 12 DSC:Failover -> ACTIVE role.
010215 18:18 Slot 12 DSC:Hub, becoming active - arb timeout
RouterA#
show redundancy
failover mode enabled, failover group = 32
Currently ACTIVE role.
DSC in slot 12:
Hub is in 'active' state.
Clock is in 'active' state.
No connection to slot 13
RouterA# reload
Proceed with reload? [confirm] y
*Feb 15 20:19:11.059:%SYS-5-RELOAD:Reload requested
System Bootstrap, Version xxx
Copyright xxx by cisco Systems, Inc.
C7200 processor with 131072 Kbytes of main memory
```

Examples

```
RouterB# show redundancy
failover mode enabled, failover group = 32
Currently BACKUP role.
No connection to slot 12
DSC in slot 13:
Hub is in 'backup' state.
Clock is in 'backup' state.
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Switching to DSC 13
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Failover:changing to active mode
*Feb 16 03:24:54.931:%DIAL13-3-MSG:
02:32:06:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:24:55.491:%OIR-6-INSCARD:Card inserted in slot 12, interfaces administratively
shut down
*Feb 16 03:24:58.455:%DIAL13-3-MSG:
02:32:09:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:25:04.939:%DIAL13-0-MSG:
RouterB# show redundancy
failover mode enabled, failover group = 32
Currently ACTIVE role.
No connection to slot 12
DSC in slot 13:
Hub is in 'active' state.
Clock is in 'backup' state.
RouterB# show redundancy history
DSC Redundancy Status Change History:
010216 03:09 Slot -1 DSC:Failover configured -> BACKUP role.
010216 03:24 Slot 13 DSC:Failover -> ACTIVE role.
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
*Feb 16 03:26:14.079:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 1 Succeeded
*Feb 16 03:26:14.255:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 3 Succeeded
*Feb 16 03:26:14.979:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 10 Succeeded
```

Examples

The following is sample output generated by this command in privileged EXEC mode on router platforms that support no keywords for the privileged EXEC mode form of the command:

```
RouterB# show redundancy
MWR1900 is the Active Router
Previous States with most recent at bottom
 INITL_INITL     Dec 31 19:00:00.000
 LISTN_INITL     Feb 28 19:00:15.568
 LISTN_LISTN     Feb 28 19:00:15.568
 SPEAK_LISTN     Feb 28 19:00:18.568
 SPEAK_SPEAK     Feb 28 19:00:18.568
 STDBY_SPEAK     Mar 19 08:54:26.191
 ACTIV_SPEAK     Mar 19 08:54:26.191
 ACTIV_STDBY     Mar 19 08:54:26.191
 ACTIV_ACTIV     Mar 19 08:54:26.191
 INITL_ACTIV     Mar 19 08:56:22.700
 INITL_INITL     Mar 19 08:56:22.700
 INITL_LISTN     Mar 19 08:56:28.544
 LISTN_LISTN     Mar 19 08:56:28.652
 LISTN_SPEAK     Mar 19 08:56:31.544
 SPEAK_SPEAK     Mar 19 08:56:31.652
 SPEAK_STDBY     Mar 19 08:56:34.544
 SPEAK_ACTIV     Mar 19 08:56:34.544
 STDBY_ACTIV     Mar 19 08:56:34.652
 ACTIV_ACTIV     Mar 19 08:56:34.652
 INITL_ACTIV     Mar 19 10:20:41.455
 INITL_INITL     Mar 19 10:20:41.455
 INITL_LISTN     Mar 19 10:20:49.243
 LISTN_LISTN     Mar 19 10:20:49.299
 LISTN_SPEAK     Mar 19 10:20:52.244
 SPEAK_SPEAK     Mar 19 10:20:52.300
 SPEAK_STDBY     Mar 19 10:20:55.244
 STDBY_STDBY     Mar 19 10:20:55.300
```

```
ACTIV_STDBY     Mar 19 10:21:01.692
ACTIV_ACTIV     Mar 19 10:21:01.692
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) router shelves (Cisco AS5800) or RSCs (Cisco AS5850).
hw-module	Enables the router shelf to stop a DSC or to restart a stopped DSC.
mode	Sets the redundancy mode.
mode y-cable	Invokes y-cable mode.
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
show chassis	Displays, for a router with two RSCs, information about mode (handover-split or classic-split), RSC configuration, and slot ownership.
show standby	Displays the standby configuration.
standalone	Specifies whether the MWR 1941-DC router is used in a redundant or standalone configuration.
standby	Sets HSRP attributes.

subscriber redundancy

To configure broadband subscriber session redundancy policy for synchronization between high availability (HA) active and standby processors, use the **subscriber redundancy** command in global configuration mode. To delete the policy, use the **no** form of this command.

subscriber redundancy [{**bulk dynamic**} **limit cpu***percentage***delay***seconds***allow***value*] [**delay***seconds*] [**rate***sessions seconds*

no subscriber redundancy

Syntax Description

bulk	(Optional) Configures a bulk synchronization redundancy policy.
dynamic	(Optional) Configures a dynamic synchronization redundancy policy.
limit cpu *percent*	(Optional) Specifies a CPU busy threshold value as a percentage. Range is 100; default is 90.
delay *seconds*	(Optional) Specifies a delay in seconds before the cluster control manager (CCM) component synchronizes sessions after the CPU busy threshold is exceeded.
allow *sessions*	(Optional) Specifies the minimum number of sessions to synchronize once the CPU busy threshold is exceeded and the specified delay is met. Range is 1 to 2147483637; default is 25.
delay *seconds*	(Optional) Specifies minimum amount of time in seconds that a session must be ready before dynamic synchronization occurs. Range is 1 to 33550.
rate *sessions seconds*	(Optional) Specifies number of sessions per time period for bulk and dynamic synchronization. • sessions--Range 1 to 32000, default is 250. • seconds--Range is 1 to 33550, default is 1.

Command Default

Subscriber redundancy policy applies default values.

Command Modes

Global configuration

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Cisco IOS HA functionality for broadband protocols and applications allows for stateful switchover (SSO) and in service software upgrade (ISSU) features that minimize planned and unplanned downtime and failures. HA uses the CCM to manage the capability to synchronize subscriber session initiation on the standby processor of a redundant processor system. Use the **subscriber redundancy** bulk command to create and modify redundancy policy used during bulk (startup) synchronization. Use the subscriber redundancy dynamic command to tune subscriber redundancy policies that throttle dynamic synchronization by monitoring CPU usage and synchronization rates. Use the subscriber redundancy delay command to establish session duration minimums for synchronization and manage dynamic synchronizing of short duration calls. Use the subscriber redundancy rate command to throttle the number of sessions to be synchronized per period.

Examples

The following example configures a 10 second delay when CPU usage exceeds 90 percent during bulk synchronization, after which 25 sessions will be synchronized before the CCM again checks CPU usage:

```
Router(config)# subscriber redundancy bulk limit cpu 90 delay 10 allow 25
```

The following example configures a minimum session duration of 15 seconds before dynamic synchronization to the standby processor:

```
Router(config)# subscriber redundancy dynamic 15
```

The following example configures 2000 sessions to be synchronized per second during bulk and dynamic synchronization:

```
Router(config)# subscriber redundancy rate 2000 1
```

Related Commands

Command	Description
show ccm sessions	Displays CCM session information.
show ppp subscriber statistics	Displays PPP subscriber statistics.
show pppatm statistics	Displays PPPoA statistics.
show pppoe statistics	Displays PPPoE statistics.

timers nsf signal

To adjust the maximum time for the initial signal timer restart period, use the timers nsf signal command in router configuration mode or address-family configuration mode. To return the signal timer to the default value, use the **no** form of this command.

timers nsf signal *seconds*

no timers nsf signal

Syntax Description

seconds	Time, in seconds, for which Enhanced Interior Gateway Routing Protocol (EIGRP) will hold routes for an inactive peer. Valid range is 10 to 30 seconds. The default is 20 seconds.

Command Default

EIGRP NSF awareness is enabled by default. EIGRP NSF awareness uses 20 seconds as the default value if this command is not configured or if the no form of this command is entered.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af)

Release	Modification
12.2(15)T	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. Address-family configuration mode was added.
12.2(33)SRE	This command was modified. 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.

Usage Guidelines

This command is entered only on a nonstop forwarding (NSF)-capable router. The EIGRP process starts a signal timer when it is notified of a switchover event. Hello packets with the RS bit set are sent during this period.

The converge timer is used to wait for the last end of table (EOT) update if all startup updates have not been received within the signal timer period. If an EIGRP process discovers no neighbor, or if it has received all startup updates from its neighbor within the signal timer period, the converge timer will not be started.

Examples

The following configuration example adjusts the signal timer value on an NSF-capable router. In the example, the signal timer is set to 30 seconds:

```
Router(config-router)# timers nsf signal 30
```

The following EIGRP named configuration example adjusts the signal timer value on an NSF-capable router. In the example, the signal timer is set to 30 seconds:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# timers nsf signal 30
```

Related Commands

Command	Description
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. This output includes NSF notifications and events.
nsf (EIGRP)	Enables or disables EIGRP NSF on an NSF-capable router.
show ip protocols	Displays the parameters and current state of the active routing protocol process. The status of EIGRP NSF configuration and support is displayed in the output.
timers nsf converge	Adjusts the maximum time that restarting router will wait for the EOT notification from an NSF-capable or NSF-aware peer.
timers nsf graceful-restart purge-time	Sets the route-hold timer to determine how long a NSF-aware router that is running EIGRP will hold routes for an inactive peer.
timers nsf route-hold	Adjusts the maximum period of time that a supporting peer will hold known routes for an NSF-capable router during a restart operation or during a well-known failure condition.

vrf (call home)

To associate a virtual routing and forwarding (VRF) instance for Call Home email message transport, use the **vrf** command in call home configuration mode. To remove the VRF association, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

name	Name of a configured VRF instance.

Command Default

No VRF is associated for Call Home. On platforms other than the Cisco ASR 1000 Series Aggregation Services Routers, the global routing table is used when this command is not configured.

Command Modes

Call home configuration (cfg-call-home)

Release	Modification
12.2(33)SXI1	This command was introduced.
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 on the Cisco ASR 1000 Series Routers.
12.2(33)SRE1	This command was integrated into Cisco IOS Release 12.2(33)SRE1 on the Cisco 7200 Series Routers.

Usage Guidelines

This command is used to configure VRF support in the Call Home feature for email transport only.

To use this command, the VRF instance must be configured on the router.

On the Cisco ASR 1000 Series Aggregation Services Routers, this command is required to support email message transport and uses the Gigabit Ethernet management interface VRF (Mgmt-intf). Therefore, to correctly use the **vrf (call-home)** command on the Cisco ASR 1000 Series Router, the Gigabit Ethernet management interface VRF must be configured.

VRF configuration for Call Home on other platforms is optional. If no VRF is specified on those platforms, the global routing table is used.

Note To configure VRF support in the Call Home feature for HTTP transport, you do not use the **vrf (call-home)** command to associate the VRF. Configure the **ip http client source-interface** command instead.

Examples

The following example shows how to associate the Mgmt-intf VRF for Call Home on the Cisco ASR 1000 Series Routers:

```
Router(config)# call-home
Router(cfg-call-home)# vrf Mgmt-intf
```

The following example shows how to associate the VRF instance for Call Home on the Cisco 7200 Series Routers:

```
Router(config)# call-home
Router(cfg-call-home)# vrf mgmt-vrf
```

Related Commands

Command	Description
call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
ip vrf forwarding (interface configuration)	Associates a VRF instance with an interface or subinterface.

vrrp sso

To enable Virtual Router Redundancy Protocol (VRRP) support of Stateful Switchover (SSO) if it has been disabled, use the **vrrp sso** command in global configuration mode. To disable VRRP support of SSO, use the **no** form of this command.

vrrp sso

no vrrp sso

Syntax Description

This command has no arguments or keywords.

Command Default

VRRP support of SSO is enabled by default.

Command Modes

Global configuration (config)

Release	Modification
12.2(33)SRC	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to enable VRRP support of SSO if it has been manually disabled by the **no vrrp sso** command.

Examples

The following example shows how to disable VRRP support of SSO:

```
Router(config)# no vrrp sso
```

Related Commands

Command	Description
debug vrrp all	Displays debugging messages for VRRP errors, events, and state transitions.
debug vrrp ha	Displays debugging messages for VRRP high availability.
show vrrp	Displays a brief or detailed status of one or all configured VRRP groups.