High Availability Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

First Published: January 11, 2013

Last Modified: January 11, 2013

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

active (call home) through http-proxy

aaa-authorization

To enable AAA authorization to run IOS commands that enable the collection of output for a Call-Home message, use the **aaa-authorization** command in call home configuration mode. To disable AAA authorization, use the **no** form of this command.

aaa-authorization [**username** *username*]

no aaa-authorization [username]

Syntax Description

username *username*	Specifies the username for authorization. Default username is callhome. Maximum length is 64.

Command Default

AAA authorization is disabled for Call-Home service as an embedded application to run IOS commands.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **aaa-authorization** command allows you to enable or disable AAA authorization when the Call-Home service is running IOS commands for the collection of output for Call-Home messages. To change the AAA authorization username, use the **aaa-authorization username** command. To change it back to the default username, use the **no** form of the **aaa-authorization username**command. After you enable AAA authorization, you must configure the Call-Home aaa-authorization username as the username on the TACACS server so that the Call-Home service can run the IOS commands.

Note When AAA authorization is disabled, you are not required to enter an AAA authorization username to send correct Call-Home messages.

Examples

The following example shows how AAA authorization is enabled:

```
Router(cfg-call-home)# aaa-authorization
```

The following example shows how AAA authorization username is changed to cisco:

```
Router(cfg-call-home)# aaa-authorization username cisco
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

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

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 Default

Command Modes

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

Command History

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.

add-command

To add IOS commands to the Snapshot alert group, use the **add-command** command in snapshot configuration mode. To remove IOS commands from the alert group, use the **no** form of this command.

add-command *command string*

no add-command *command string*

Syntax Description

command string	IOS command. Maximum length is 128. **Note** The IOS command string must be enclosed in quotes (“”) if it contains white spaces.

Command Default

The Snapshot alert group has no command to run.

Command Modes

Snapshot configuration (cfg-call-home-snapshot)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

When you add commands to the Snapshot alert group, the output of the commands added are included in the snapshot message.

Examples

The following example shows the **show version** command added to the snapshot alert group:

```
Router(cfg-call-home-snapshot)# add-command “show version”
```

Related Commands

Command	Description
alert-group-config snapshot	Enters snapshot configuration mode.

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)

Command History

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

Usage Guidelines

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.

alert-group-config snapshot

To enter snapshot configuration mode to enable the addition of IOS commands to the Snapshot alert group, use the **alert-group-config snapshot** command in call home configuration mode. To remove all IOS commands from the Snapshot alert group, use the **no** form of this command.

alert-group-config snapshot

no alert-group-config snapshot

Syntax Description

This command has no arguments or keywords.

Command Default

No IOS commands are added to the Snapshot alert group.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example shows how to enter snapshot configuration mode:

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

Related Commands

Command	Description
add-command	Adds IOS commands to the Snapshot alert group.
call-home	Enters call home configuration mode.

anonymous-reporting-only

To set the TAC profile to anonymous mode, use the **anonymous-reporting-only** command in TAC profile configuration mode. To disable anonymous reporting, use the **no** form of this command.

anonymous-reporting-only

no anonymous-reporting-only

Syntax Description

This command has no arguments or keywords.

Command Default

Anonymous reporting is disabled. TAC profile sends a full report of all types of events subscribed in the profile.

Command Modes

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

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

When anonymous-reporting-only is set, only crash, inventory, and test messages are sent.

Examples

The following example shows how TAC profile is set to anonymous mode:

```
Router(cfg-call-home-profile)# anonymous-reporting-only
```

Related Commands

Command	Description
profile	Enables TAC profile configuration mode.

call-home (global configuration)

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

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you use the **call-home** command, you enter call home configuration mode and you can configure settings for the Call Home feature in your system.

When a call home message is sent only to a call home back-end server, the server checks the output length of each message. If the message length exceeds 10KB, the server compresses the output length. If the compressed message length still exceeds 10KB, the server drops the message.

Examples

The following example shows how to enter call home configuration mode and lists the commands that are available for Call Home configuration depending on your release:

```
Device(config)# call-home

Device(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 reporting

To enable Smart Call Home service with full reporting or anonymous reporting, use the **call-home reporting** command in global configuration mode.

call-home reporting {**anonymous**| **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address*| *ipv6-address*| *name*} **port** *port-number*]

Syntax Description

anonymous	Enables Call-Home TAC profile to only send crash, inventory, and test messages and send the messages in an anonymous way.
contact-email-addr *email-address*	Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process.
http-proxy {*ipv4-address*| *ipv6-address* | *name*}	(Optional) IP (ipv4 or ipv6) address or name of proxy server. Maximum length is 64.
port *port-number*	(Optional) Port number. Range: 1 to 65535.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out.

The **call-home reporting** command is not present in running or startup configuration files and there is no support for the no form of this command.

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

no service call-home

To remove the assigned e-mail address, use the **no** form of the **contact-email-addr** in call home configuration mode.

no contact-email-addr *email-address*

The HTTP proxy option allows you to make use of your own proxy server to buffer and secure Internet connections from your devices.

To disable the specified HTTP proxy server and port for the HTTP request, use the **no** form of the **http-proxy** command in call home configuration mode.

no http-proxy

To disable a destination profile, use the **no** form of the **active** command in call home profile configuration mode.

no active

To disable the CiscoTac-1 predefined profile, use the **default** form of the **active** command in call home profile configuration mode.

default active

If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. For more information, see Configuring Call Home for Cisco Integrated Service Routers .

To disable anonymous reporting, use the **no** form of the **anonymous-reporting-only**command in TAC profile configuration mode.

no anonymous-reporting-only

Examples

The following example shows the Call-Home TAC profile enabled for all alert group messages, allowing it to send a full inventory message to start Smart Call Home registration:

Router(config)# **call-home reporting contact-email-addr email@company.com**

The following example shows the Call-Home TAC profile enabled to send crash, inventory, and test messages anonymously to port 1 of proxy server 1.1.1.1:

```
Router(config)# call-home reporting anonymous http-proxy 1.1.1.1 port 1
```

call-home request

To submit information about your system to Cisco for report and analysis information, use the **call-home request** command in privileged EXEC mode.

call-home request {**bugs-list**| **command-reference**| **config-sanity**| **output-analysis** "*show-command*"| **product-advisory**} {**profile** *name* [**ccoid** *user-id*]| **ccoid** *user-id* [**profile** *name*]}

Syntax Description

bugs-list	Requests report of known bugs in the running version and in the currently applied features.
command-reference	Requests report of reference links to all commands in the running configuration.
config-sanity	Requests report of information on best practices related to the current running configuration.
output-analysis " *show-command* "	Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (" ").
product-advisory	Requests report of Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.
profile *name*	Specifies an existing Call Home destination profile to which the request is sent. If no profile is specified, the request is sent to the CiscoTAC-1 profile.
ccoid *user-id*	Specifies the identifier of a registered Smart Call Home user. If a *user-id* is specified, the resulting analysis report is sent to the e-mail address of the registered user. If no *user-id* is specified, the report is sent to the contact e-mail address of the device.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

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

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When you use this command, an analysis report is sent by Cisco to a configured contact e-mail address. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.

Based on the keyword option specified, the output of a predetermined set of commands as applicable to your system such as the **show running-config all**, **show version**, and **show module** (standalone) or **show module switch all**(VS system) commands, is sent to Cisco for analysis.

Examples

The following example shows a request for analysis of the **show diagnostic result module all** command to be sent to the contact information specified for the Call Home destination profile named “TG”:

```
Router# call-home request output-analysis "show diagnostic result module all" profile TG
```

The following example shows a request for the known bugs list to be sent to the Call Home destination profile named “CiscoTAC-1” and a registered CCO userid “myuserid”:

```
Router# call-home request bugs-list profile CiscoTAC-1 ccoid myuserid
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
call-home send	Executes an EXEC-level CLI command and sends the command output for Call Home using e-mail.
call-home send alert-group	Manually sends an alert group message for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.

call-home send

To execute an EXEC-level CLI command and send the command output for Call Home using e-mail, use the **call-home send** command in privileged EXEC mode.

call-home send *"exec-command"* {**email** *email-addr* [**tac-service-request** *request-number*]| **tac-service-request** *request-number* [**email** *email-addr*]}

Cisco 7600 Series Routers in Cisco IOS Release 12.2(33)SRC

call-home send *"exec-command"* {**email** *email-addr* [**service-number** *SR*]| **service-number** *SR*}

Syntax Description

“ *exec-command* ”	Specifies an EXEC-level CLI command to be executed. The command output is sent by e-mail. The EXEC command must be contained in quotes (“ “).
email *email-addr*	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number *SR*	(Cisco 7600 Series Routers in Cisco IOS Release 12.2(33)SRC) Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.
tac-service-request *request-number*	Specifies the TAC service request number that appears in the subject line of the e-mail. This keyword is optional if used after entering the **email** option.

Command Default

This command has no default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. The **service-number**keyword option is replaced by the **tac-service-request** keyword option.

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The command must be enclosed in quotes (“ ”), and can be any EXEC-level command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com. The e-mail will be sent in long text format with the service number, if specified, in the subject line.

Examples

This example shows how to send a CLI command and have the command output e-mailed:

```
Router# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
call-home send alert-group	Manually sends an alert group message for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.

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

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

Cisco ASR 1000 Series Aggregation Services Routers

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

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
crash	Sends the system crash message with the latest crash information to the destination profile.
diagnostic module *number*	Sends the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay number. The *number* value can be the module number, the slot/subslot number, or the slot/bay number. This option is supported on the Cisco Catalyst 4500 series switch, the Cisco Catalyst 6500 series switch, and the Cisco 7600 series router.
diagnostic slot *number*	Sends the diagnostic alert-group message to destination profiles for the specified slot, such as R0 for Route Processor (RP) slot 0. This option is supported on the Cisco ASR 1000 series router.
inventory	Sends the inventory call-home message to the destination profile.
profile *profile-name*	(Optional) Specifies the name of the destination profile.

Command Default

A Call Home alert group message is not sent manually.

Command Modes

Privileged EXEC (#)

Command History

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

Release	Modification
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. The **diagnostic slot** keyword was added.
15.2(3)T	This command was modified. The **crash** keyword was added.

Usage Guidelines

The Cisco ASR 1000 series router does not support the **diagnostic module** keyword. Instead, use the **diagnostic slot** keyword.

If you do not specify the keyword-argument pair **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, crash, diagnostic, and inventory alert group messages can be sent manually.

Examples

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

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

The following example shows how to send a system crash message with the latest crash information to a destination profile:

```
Device# call-home send alert-group crash
```

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

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

The following example shows how to send a diagnostic alert-group message to a destination profile named profile1 for a specific module, slot/subslot, or slot/bay number:

```
Device# call-home send alert-group diagnostic module 3/2 profile profile1
```

The following example shows how to send a diagnostic alert-group message to a destination profile named profile1 on RP slot 0 on a Cisco ASR 1000 Series Router:

```
Device# call-home send alert-group diagnostic slot R0 profile profile1
```

The following example shows how to send an inventory call-home message to a destination profile:

```
Device# 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 the Call Home feature.
show call-home	Displays the Call Home configuration information.

call-home test

To manually send a Call Home test message to a destination profile, use the **call-home test** command in privileged EXEC mode.

call-home test [**"***test-message***"**] **profile** *profile-name*

Syntax Description

“ *test-message* ”	(Optional) Test message text enclosed in required quotation marks (“ “).
profile *profile-name*	Specifies the name of the destination profile.

Command Default

This command has no default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command sends a test message to the specified destination profile. If you enter test message text, you must enclose the text in quotes (“ ”) if it contains spaces. If you do not enter a message, a default message is sent.

Examples

The following example shows how to manually send a Call Home test message with the text “test of the day” to the profile named CiscoTAC-1:

```
Router# call-home test “test of the day” profile CiscoTAC-1
```

Related Commands

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

call-home send alert-group	Manually sends an alert group message for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.

clear ip rsvp high-availability counters

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

clear ip rsvp high-availability counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **clear ip rsvp high-availability counters**command to clear (set to zero) the HA counters, which include state, resource failures, and historical information.

Examples

The following example clears all the HA information currently being maintained by the RP:

```
Router# clear ip rsvp high-availability counters
```

Related Commands

Command	Description
show ip rsvp high-availability counters	Displays the RSVP TE HA counters that are being maintained by an RP.

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)

Command History

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

Usage Guidelines

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)

Command History

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

Usage Guidelines

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)

Command History

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

Usage Guidelines

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.

crashdump-timeout

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

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

no crashdump-timeout

Syntax Description

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

Command Default

The default timeout for this command is 5 minutes.

Command Modes

Redundancy

Command History

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

Usage Guidelines

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

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

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

Note The core dump process adds the slot number to the core dump file to identify which processor generated the file content. For more information on how to configure the system for a core dump, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* , Release 12.4.

Examples

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

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

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)

Command History

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

Usage Guidelines

The **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.

data-privacy

To scrub data from running configuration files to protect the privacy of users, use the **data-privacy** command in call home configuration mode. To revert back to data privacy default configuration, use the **no** form of this command.

data-privacy {**level** {**normal**| **high**}| **hostname**}

no data-privacy {**level**| **hostname**}

Syntax Description

level	Specifies the level of commands to be scrubbed.
normal	Scrubs all normal-level commands. This is the default data-privacy level.
high	Scrubs all normal-level commands plus the IP domain name and IP address commands.
hostname	Scrubs all high-level or normal-level commands plus the **hostname** command. **Note** Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Command Default

Default level is normal and hostname scrubbing is disabled. Password/secret and other commands are scrubbed from running configuration files.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **data-privacy** command scrubs data, such as IP addresses, from running configuration files to protect the privacy of customers. For Cisco IOS Release 15.2(2)T and earlier releases, the output of show commands are not being scrubbed except for configuration messages in the **show running-config all** and **show startup-config** data.

Note Enabling the **data-privacy** command can affect CPU utilization when scrubbing a large amount of data.

Examples

The following example shows how to scrub all normal-level commands plus the IP domain name and IP address commands from the running configuration file:

```
Router(cfg-call-home)# data-privacy level high
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

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)

Command History

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

Usage Guidelines

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.

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

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

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration

Command History

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

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

Examples

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

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

Related Commands

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

http-proxy

To specify the HTTP proxy server and port for the HTTP request and prevent the device from connecting to Cisco or other destinations using HTTP directly, use the **http-proxy** command in call home configuration mode. To disable, use the **no** form of this command.

http-proxy {*ipv4-address*| *ipv6-address*| *name*} **port** *port-number*

no http-proxy

Syntax Description

ipv4-address | *ipv6-address* | *name*	IP (ipv4 or ipv6) address or name of proxy server. Maximum length is 64.
port *port-number*	Port number. Range: 1 to 65535.

Command Default

No HTTP proxy server is used for Call-Home messages.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example specifies port 1 of proxy server 1.1.1.1 as the HTTP proxy server port for the HTTP request:

```
Router(cfg-call-home)# http-proxy 1.1.1.1 port 1
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

mail-server through service image-version efsu

nsf (OSPF)

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

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

nsf [**enforce global**]

no nsf [**enforce global**]

Syntax Description

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

Command Default

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

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

nsf cisco

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

nsf cisco [**enforce global**| **helper** [**disable**]]

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

Syntax Description

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

Command Default

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

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
nsf ietf	Enables IETF NSF.

nsf ietf

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

nsf ietf [**restart-interval** *seconds*| **helper** [**disable**| **strict-lsa-checking**]]

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

Syntax Description

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

Command Default

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

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF.

show call-home through vrrp sso

show cef nsf

To show the current Cisco nonstop forwarding (NSF) state of Cisco Express Forwarding on both the active and standby Route Processors (RPs), use the **s how cef nsf**command in privileged EXEC mode.

show cef nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Command History

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

If you enter the **show cef nsf** command before a switchover occurs, no switchover activity is reported. After a switchover occurs, you can enter the **show cef nsf** command to display details about the switchover as reported by the newly active RP. On the Cisco 12000 and 7500 series Internet routers, details about line card switchover are also provided.

Examples

The following example shows the current NSF state:

```
Router# show cef nsf
Last switchover occurred:        00:01:30.088 ago
 Routing convergence duration:   00:00:34.728
 FIB stale entry purge durations:00:00:01.728 - Default
                                  00:00:00.088 - Red
          Switchover
 Slot    Count   Type   Quiesce Period
 1           2    sso   00:00:00.108
 2           1   rpr+   00:00:00.948
 3           2    sso   00:00:00.152
 5           2    sso   00:00:00.092
 6          1   rpr+   00:00:00.632
 No NSF stats available for the following linecards:4 7
```

The table below describes the significant fields shown in the display.

Table 1: show cef nsf Field Descriptions

Field	Description
Last switchover occurred	Time since the last system switchover.
Routing convergence duration	Time taken after the switchover before the routing protocol signaled Cisco Express Forwarding that they had converged.
Stale entry purge	Time taken by Cisco Express Forwarding to purge any stale entries in each FIB table. In the example, these are the FIB tables names "Default" and "Red."
Switchover	Per-line card NSF statistics.
Slot	Line card slot number.
Count	Number of times the line card has switched over. This value will always be 1, unless the type is SSO.
Type	Type of switchover the line card performed last. The type can be SSO, RPR+ or RPR.
Quiesce Period	Period of time when the line card was disconnected from the switching fabric. During this time, no packet forwarding can take place. Other system restart requirements may add additional delay until the line card can start forwarding packets.

Related Commands

Command	Description
clear ip cef epoch	Begins a new epoch and increments the epoch number for a Cisco Express Forwarding table.
show cef state	Displays the state of Cisco Express Forwarding on a networking device.

show cef state

To display the state of Cisco Express Forwarding on a networking device, use the **show cef state**command in privileged EXEC mode.

show cef state

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.
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 for the Cisco 7304 router was added. 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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

Examples

The following example shows the state of Cisco Express Forwarding on the active Route Processor (RP):

```
Router# show cef state
CEF Status:
 RP instance
 common CEF enabled
IPv4 CEF Status:
 CEF enabled/running
 dCEF disabled/not running
 CEF switching enabled/running
 universal per-destination load sharing algorithm, id A189DD49
IPv6 CEF Status:
 CEF enabled/running
 dCEF disabled/not running
 original per-destination load sharing algorithm, id A189DD49
```

The table below describes the significant fields shown in the display.

Table 2: show cef state Field Description (New)

Field	Description
RP instance	Cisco Express Forwarding status is for the RP.
common CEF enabled	Common Cisco Express Forwarding is enabled.
IPv4 CEF Status	Cisco Express Forwarding mode and status is for IPv4.
universal per-destination load sharing algorithm	IPv4 is using the universal per-destination load sharing algorithm for Cisco Express Forwarding traffic.
IPv6 CEF Status	Cisco Express Forwarding mode and status is for IPV6.
original per-destination load sharing algorithm	IPv6 is using the original per-destination load sharing algorithm for Cisco Express Forwarding traffic.

Examples

The following example shows the state of Cisco Express Forwarding on the active Route Processor (RP):

```
Router# show cef state
RRP state:
     I am standby RRP:           no
     RF Peer Presence:           yes
     RF PeerComm reached:        yes
     Redundancy mode:            SSO(7)
     CEF NSF:                    enabled/running
```

The table below describes the significant fields shown in the display.

Table 3: show cef state Field Descriptions

Field	Description
I am standby RRP: no	This RP is not the standby.
RF Peer Presence: yes	This RP does have RF peer presence.
RF PeerComm reached: yes	This RP has reached RF peer communication.
Redundancy mode: SSO(&)	Type of redundancy mode on this RP.
CEF NSF: enabled/running	States whether Cisco Express Forwarding nonstop forwarding (NSF) is running or not.

The following example shows the state of Cisco Express Forwarding on the standby RP:

```
Router# show cef state
```

```
RRP state:
     I am standby RRP:           yes
     My logical slot:            0
     RF Peer Presence:           yes
     RF PeerComm reached:        yes
     CEF NSF:                    running
```

Related Commands

Command	Description
clear ip cef epoch	Begins a new epoch and increments the epoch number for a Cisco Express Forwarding table.
show cef nsf	Displays the current NSF state of Cisco Express Forwarding on both the active and standby RPs.

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 (#)

Command History

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
```

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)

Command History

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.