

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 <i>name</i> }	(Optional) Displays configuration information for Call Home destination profiles, where: <ul style="list-style-type: none"> • all—Displays information for all configured profiles. • <i>name</i>—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 (#)

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

Examples The following example 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 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 **show 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.
	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

[Table 1](#) 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 **Example for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases**
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
```

[Table 3](#) 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.

Example for Cisco IOS Releases Before Cisco IOS 12.2(25)S

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
```

Table 3 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 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 vpnv4 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

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
	Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

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 4 describes the significant fields shown in the display.

Table 4 *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 (#)

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
```

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 (#)

Command History	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 5](#) describes the significant fields shown in the display.

Table 5 *show ip rsvp high-availability counters—Active RP Field Descriptions*

Field	Description
State	The RP state: <ul style="list-style-type: none"> Active—Active RP.
Bulk sync	The number of requests made by the standby RP to the active RP to resend all write database entries: <ul style="list-style-type: none"> Initiated—The number of bulk sync operations initiated by the standby RP since reboot.
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: <ul style="list-style-type: none"> 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.
Failed to Start	The number of negotiations that failed to start.

Table 5 *show ip rsvp high-availability counters—Active RP Field Descriptions (continued)*

Field	Description
Messages	The number of negotiation messages sent and received. These messages can be succeeded or failed. <ul style="list-style-type: none"> • 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 6 describes the significant fields shown in the display.

Table 6 show ip rsvp high-availability counters—Standby RP Field Descriptions

Field	Description
State	The RP state: <ul style="list-style-type: none"> Standby—Standby (backup) RP.
Checkpoint Messages (Items) Received	The details of the messages or items received by the standby RP. Values are the following: <ul style="list-style-type: none"> 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 5 .
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.
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 ip rsvp interface detail

To display the hello configuration for specific interfaces, use the **show ip rsvp interface detail** command in user EXEC or privileged EXEC mode.

show ip rsvp interface detail [*type number*]

Syntax Description	<i>type number</i>	(Optional) Type and number of the interface for which you want to display the hello configuration.
---------------------------	--------------------	--

Command Default If the optional argument is not specified, the hello configuration for all interfaces is displayed.

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

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
	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)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
	12.2(33)SRE	This command was modified. The output was updated to display the source address used in the PHOP address field.
	15.1(2)T	This command was modified. The output was updated to display the overhead percent.

Examples

The following is sample output from the **show ip rsvp interface detail** command:

```
Router# show ip rsvp interface detail GigabitEthernet 9/47

Tu0:
  RSVP: Enabled
  Interface State: Up
  Bandwidth:
    Curr allocated: 10K bits/sec
    Max. allowed (total): 75K bits/sec
    Max. allowed (per flow): 75K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total): 0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
    Tunnel IP Overhead percent:
      4
    Tunnel Bandwidth considered:
```

```

Yes
Traffic Control:
  RSVP Data Packet Classification is ON via CEF callbacks
Signalling:
  DSCP value used in RSVP msgs: 0x3F
  Number of refresh intervals to enforce blockade state: 4
Authentication: disabled
  Key chain: <none>
  Type: md5
  Window size: 1
  Challenge: disabled
Hello Extension:
  State: Disabled
  
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip rsvp interface detail Field Descriptions

Field	Description
RSVP	Status of the Resource Reservation Protocol (RSVP) protocol (Enabled or Disabled).
Interface State	Status of the interface (Up or Down).
Curr allocated	Amount of bandwidth (in bits per second [bps]) currently allocated.
Max. allowed (total)	Total maximum amount of bandwidth (in bps) allowed.
Max. allowed (per flow)	Maximum amount of bandwidth (in bps) allowed per flow.
Max. allowed for LSP tunnels using sub-pools	Maximum amount of bandwidth permitted for label switched path (LSP) tunnels that obtain their bandwidth from subpools.
Tunnel IP Overhead Percent	Overhead percent to override the RSVP bandwidth manually.
Tunnel Bandwidth Considered	Indicates if the tunnel bandwidth is considered.
DSCP value used in RSVP msgs	Differentiated services code point (DSCP) value that is in RSVP messages.
Source address of outgoing RSVP messages	Source address used in the PHOP address field of the outgoing RSVP messages.
BFD Extension State	State (Enabled or Disabled) of Bidirectional Forwarding Detection (BFD) extension.
RSVP Hello Extension State	State (Enabled or Disabled) of hello extension.
Missed Acks	Number of sequential acknowledgments that the node did not receive.
DSCP in HELLOs	DSCP value that is in hello messages.

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the hello message sent out from an interface.
ip rsvp signalling hello refresh interval	Configures the hello request interval.

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

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

Usage Guidelines The **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 8](#) describes the significant fields shown in the display.

Table 8 *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.

Table 8 *show isis nsf Field Descriptions (continued)*

Field	Description
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 slot all		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 eFSU data.

Command Default None

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

Command History	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 clients

To display a list of the current In Service Software Upgrade (ISSU) clients—that is, the network applications and protocols supported by ISSU—use the **show issu clients** command in user EXEC or privileged EXEC mode.

show issu clients

Syntax Description This command has no arguments or keywords.

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

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	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 This command lists all ISSU clients currently operating in the network, along with their Client ID numbers and the number of entities each client contains.

You should enter this command before you enter the **issu runversion** command, because if a client (application or protocol) that needs to continue operating in the network does not appear in the displayed list, you will know not to continue the software upgrade (because proceeding further with ISSU would then halt the operation of that application or protocol).

Examples The following example shows a client list displayed by entering this command:

```
Router# show issu clients

Client_ID = 2, Client_Name = ISSU Proto client, Entity_Count = 1
Client_ID = 3, Client_Name = ISSU RF, Entity_Count = 1
Client_ID = 4, Client_Name = ISSU CF client, Entity_Count = 1
Client_ID = 5, Client_Name = ISSU Network RF client, Entity_Count = 1
Client_ID = 7, Client_Name = ISSU CONFIG SYNC, Entity_Count = 1
Client_ID = 8, Client_Name = ISSU ifIndex sync, Entity_Count = 1
Client_ID = 9, Client_Name = ISSU IPC client, Entity_Count = 1
Client_ID = 10, Client_Name = ISSU IPC Server client, Entity_Count = 1
Client_ID = 11, Client_Name = ISSU Red Mode Client, Entity_Count = 1
Client_ID = 12, Client_Name = ISSU ESHA services client, Entity_Count = 1
Client_ID = 100, Client_Name = ISSU rfs client, Entity_Count = 1
Client_ID = 110, Client_Name = ISSU ifs client, Entity_Count = 1
Client_ID = 1001, Client_Name = OC3POS-6, Entity_Count = 4
Client_ID = 1002, Client_Name = C10K ATM, Entity_Count = 1
Client_ID = 1003, Client_Name = C10K CHSTM1, Entity_Count = 1
Client_ID = 1004, Client_Name = C10K CT3, Entity_Count = 1
Client_ID = 1005, Client_Name = C10K GE, Entity_Count = 1
Client_ID = 1006, Client_Name = C10K ET, Entity_Count = 1
```

```

Client_ID = 1007, Client_Name = C10K CHE1T1, Entity_Count = 1
Client_ID = 1009, Client_Name = C10K MFE, Entity_Count = 1
Client_ID = 1010, Client_Name = C10K APS, Entity_Count = 1
Client_ID = 1013, Client_Name = C10K CARD OIR, Entity_Count = 1
Client_ID = 2002, Client_Name = CEF Push ISSU client, Entity_Count = 1
Client_ID = 2003, Client_Name = ISSU XDR client, Entity_Count = 1
Client_ID = 2004, Client_Name = ISSU SNMP client, Entity_Count = 1
Client_ID = 2005, Client_Name = ISSU HDLC Client, Entity_Count = 1
Client_ID = 2006, Client_Name = ISSU QoS client, Entity_Count = 1
Client_ID = 2007, Client_Name = ISSU LSD Label Mgr HA Client, Entity_Count = 1
Client_ID = 2008, Client_Name = ISSU Tableid Client, Entity_Count = 1
Client_ID = 2009, Client_Name = ISSU MPLS VPN Client, Entity_Count = 1
Client_ID = 2010, Client_Name = ARP HA, Entity_Count = 1
Client_ID = 2011, Client_Name = ISSU LDP Client, Entity_Count = 1
Client_ID = 2012, Client_Name = ISSU HSRP Client, Entity_Count = 1
Client_ID = 2013, Client_Name = ISSU ATM Client, Entity_Count = 1
Client_ID = 2014, Client_Name = ISSU FR Client, Entity_Count = 1
Client_ID = 2015, Client_Name = ISSU REDSSOC client, Entity_Count = 1
Client_ID = 2019, Client_Name = ISSU TCP client, Entity_Count = 1
Client_ID = 2020, Client_Name = ISSU BGP client, Entity_Count = 1
Client_ID = 2021, Client_Name = XDR Int Priority ISSU client, Entity_Count = 1
Client_ID = 2022, Client_Name = XDR Proc Priority ISSU client, Entity_Count = 1
Client_ID = 2023, Client_Name = FIB HWIDB ISSU client, Entity_Count = 1
Client_ID = 2024, Client_Name = FIB IDB ISSU client, Entity_Count = 1
Client_ID = 2025, Client_Name = FIB HW subblock ISSU client, Entity_Count = 1
Client_ID = 2026, Client_Name = FIB SW subblock ISSU client, Entity_Count = 1
Client_ID = 2027, Client_Name = Adjacency ISSU client, Entity_Count = 1
Client_ID = 2028, Client_Name = FIB IPV4 ISSU client, Entity_Count = 1
Client_ID = 2030, Client_Name = MFI Pull ISSU client, Entity_Count = 1
Client_ID = 2031, Client_Name = MFI Push ISSU client, Entity_Count = 1
Client_ID = 2051, Client_Name = ISSU CCM Client, Entity_Count = 1
Client_ID = 2052, Client_Name = ISSU PPP SIP CCM Client, Entity_Count = 1
Client_ID = 2054, Client_Name = ISSU process client, Entity_Count = 1

```

Base Clients:

```

Client_Name = ISSU Proto client
Client_Name = ISSU RF
Client_Name = ISSU CF client
Client_Name = ISSU Network RF client
Client_Name = ISSU CONFIG SYNC
Client_Name = ISSU ifIndex sync
Client_Name = ISSU IPC client
Client_Name = ISSU IPC Server client
Client_Name = ISSU Red Mode Client
Client_Name = ISSU EHSA services client

```

Table 8 describes the significant fields shown in the display.

Table 9 *show issu clients Field Descriptions*

Field	Description
Client_ID	The identification number used by ISSU for that client.
Client_Name	A character string describing the client. “Base Clients” are a subset, which includes: <ul style="list-style-type: none"> • Inter-Process Communications (IPC) • Redundancy Framework (RF) • Checkpoint Facility (CF) • Cisco Express Forwarding • Network RF (for IDB stateful switchover) • EHSAs Services (including ifIndex) • Configuration Synchronization.
Entity_Count	The number of entities within this client. An entity is a logical group of sessions with some common attributes.

Related Commands

Command	Description
show issu message types	Displays the formats, versions, and size of ISSU messages supported by a particular client.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu comp-matrix

To display information regarding the In Service Software Upgrade (ISSU) compatibility matrix, use the **show issu comp-matrix** command in user EXEC or privileged EXEC mode.

```
show issu comp-matrix { negotiated | stored }
```

Syntax Description

negotiated	Displays negotiated matrix information.
stored	Displays stored matrix information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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)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

Before attempting an ISSU, you should know the compatibility level between the Cisco IOS software versions on the active and the standby Route Processors (RPs). ISSU will not work if the two versions are incompatible. Use the **show issu comp-matrix** command with the **negotiated** keyword to display information on the negotiation of the compatibility matrix data between two software versions on a given system.

Compatibility matrix data is stored with each Cisco IOS software image that supports the ISSU capability. Use the **show issu comp-matrix** command with the **stored** keyword to display stored compatibility matrix information.

Examples

The following example shows how to display stored compatibility matrix information:

```
Router# show issu comp-matrix stored
```

show issu entities

To display information about entities within one or more In Service Software Upgrade (ISSU) clients, use the **show issu entities** command in user EXEC or privileged EXEC mode.

show issu entities [*client-id*]

Syntax Description

client-id (Optional) The identification number of a single ISSU client.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

An entity is a logical group of sessions that possess some common attributes. Enter a Client_ID if you are interested in seeing information only about one client’s entities. If a Client_ID is not specified, the command will display all ISSU clients’ entities known to the device.

If you are not sure of the precise Client_ID number to enter for the client you are interested in, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example shows detailed information about the entities within the virtual routing and forwarding (VRF) (“Table ID”) client:

```
Router# show issu entities 2008

Client_ID = 2008 :
  Entity_ID = 1, Entity_Name = Tableid Entity :
    MsgType MsgGroup CapType CapEntry CapGroup
    Count   Count   Count   count   Count
    2       2       1       2       2
```

Table 10 describes the significant field shown in the display.

Table 10 *show issu entities Field Descriptions*

Field	Description
Client_ID	The identification number used by ISSU for the specified client.
Entity_ID	The identification number used by ISSU for each entity within this client.
Entity_Name	A character string describing the entity.
MsgType Count	The number of message types within the identified entity.

Table 10 *show issu entities Field Descriptions (continued)*

Field	Description
MsgGroup Count	The number of message groups within the identified entity. A message group is a list of message types.
CapType Count	The number of capability types within the identified entity.
CapEntry Count	The number of capability entries within the identified entity. A capability entry is a list of all mutually dependent capability types within a particular client session and, optionally, other capability types belonging to that client session.
CapGroup Count	The number of capability groups within the identified entity. A capability group is a list of capability entries given in priority sequence.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications and protocols on this network supported by ISSU.
show issu sessions	Displays detailed information about a particular ISSU client—including whether the client status for the impending software upgrade is COMPATIBLE.

show issu message types

To display formats (“types”), versions, and maximum packet size of the In Service Software Upgrade (ISSU) messages supported by a particular client, use the **show issu message types** command in user EXEC or privileged EXEC mode.

show issu message types *client-id*

Syntax Description

client-id The identification number used by ISSU for a client application.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

If you are not sure of the Client_ID number to enter into this command, use the **show issu clients** command. It displays the current list of clients, along with their names and ID numbers.

Examples

The following example displays the message type, version, and maximum message size supported by the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) client:

```
Router# show issu message types 2009

Client_ID = 2009, Entity_ID = 1 :
  Message_Type = 1, Version_Range = 1 ~ 1
    Message_Ver = 1, Message_Mtu = 32
```

[Table 11](#) describes the significant fields shown in the display.

Table 11 *show issu message types Field Descriptions*

Field	Description
Client_ID	The identification number used by ISSU for this client.
Entity_ID	The identification number used by ISSU for this entity.
Message_Type	An identification number that uniquely identifies the format used in the ISSU messages conveyed between the two endpoints.
Version_Range	The lowest and highest message-version numbers contained in the client application.

Table 11 *show issu message types Field Descriptions (continued)*

Field	Description
Message_Ver	Message version. Because each client application contains one or more versions of its messages, ISSU needs to discover these versions and negotiate between the new and old system software which version to use in its preparatory communications.
Message_Mtu	Maximum size (in bytes) of the transmitted message. A value of 0 means there is no restriction on size; fragmentation and reassembly are therefore being handled in a manner transparent to the ISSU infrastructure.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications on this network supported by ISSU.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu negotiated

To display details of the session’s negotiation about message version or client capabilities, use the **show issu negotiated** command in user EXEC or privileged EXEC mode.

show issu negotiated {**version** | **capability**} *session-id*

Syntax Description	version	capability	session-id
	Displays results of a negotiation about versions of the messages exchanged during the specified session, between the active and standby endpoints.	Displays results of a negotiation about the client application’s capabilities for the specified session.	The number used by In Service Software Upgrade (ISSU) to identify a particular communication session between the active and the standby devices.

Command Modes
 User EXEC
 Privileged EXEC

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines
 If you are not sure of the session_ID number to enter into this command, enter the **show issu sessions** command. It will display the session_ID.

Examples
 The following example displays the results of a negotiation about message versions:

```
router# show issu negotiated version 39

Session_ID = 39 :
    Message_Type = 1, Negotiated_Version = 1, Message_MTU = 32
```

Table 12 describes the significant fields shown in the display.

Table 12 *show issu negotiated version Field Descriptions*

Field	Description
Session_ID	The identification number of the session being reported on.
Message_Type	An identification number that uniquely identifies the format that was used by the ISSU messages conveyed between the two endpoints.

Table 12 *show issu negotiated version Field Descriptions (continued)*

Field	Description
Negotiated_Version	The message version that was decided upon, for use during the software upgrade process.
Message_Mtu	Maximum size (in bytes) of the transmitted message. A value of 0 means there is no restriction on size. In that case, fragmentation and reassembly are handled in a manner transparent to the ISSU infrastructure.

The following example displays the results of a negotiation about the client application's capabilities:

```
router# show issu negotiated capability 39
```

```
Session_ID = 39 :
    Negotiated_Cap_Entry = 1
```

Table 13 describes the significant fields shown in the display.

Table 13 *show issu negotiated capability Field Descriptions*

Field	Description
Session_ID	The identification number of the session being reported on.
Negotiated_Cap_Entry	A numeral that stands for a list of the negotiated capabilities in the specified client session.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications on this network supported by ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu outage

To display the maximum outage time for installed line cards during an in service software upgrade (ISSU), use the **show issu outage** command from the switch processor (SP) console.

```
show issu outage slot {slot-num | all}
```

Syntax Description

<i>slot-num</i>	Displays the maximum outage time for the line card in the specified slot.
all	Displays the maximum outage time for all installed line cards.

Command Modes

SP console

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on Cisco 7600 series routers.

Usage Guidelines

Once the new software is downloaded onto the router (after you issue the **issu loadversion** command), you can issue **show issu outage slot all** from the SP console to display the maximum outage time for installed line cards.

During an ISSU, the router preloads line card software onto line cards that support enhanced Fast Service Upgrade (eFSU). Then, when the switchover occurs between active and standby processors, the line cards that support eFSU are restarted with the new, preloaded software, which helps to minimize outage time during the upgrade. Line cards that do not support eFSU undergo a hard reset at switchover, and the software image is loaded after the line card is restarted.

The output for the **show issu outage** command shows the type of reload that the line card will perform along with the maximum outage time (see the “Examples” section).



Note

In the MDR Mode field of the command output, NSF_RELOAD indicates that the line card will not be reloaded, which means that outage time will be 0 to 3 seconds. NSF_RELOAD applies only to ISSU upgrades between two software releases that have the same line card software.

Examples

The following command examples show the maximum outage time for installed line cards:

```
Router# show issu outage slot all
```

```
Slot # Card Type                               MDR Mode      Max Outage Time
-----
  1 CEF720 4 port 10-Gigabit Ethernet          NSF_RELOAD    3 secs
  2 FRU type (0x6003, 0x3F8(1016))             NSF_RELOAD    3 secs
  3 4-subslot SPA Interface Processor-200      NSF_RELOAD    3 secs
```

```
Router#
```

```
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#

Table 5 describes the fields in the display.

Table 14 *show issu outage Field Descriptions*

Field	Description
Slot	The chassis slot number in which the line card is installed.
Card Type	The type of line card installed in the slot.
MDR Mode	The type of software reload that the line card will perform after the ISSU switchover: <ul style="list-style-type: none"> • NSF_RELOAD indicates that the line card will undergo an SSO/NSF type of switchover, which means that the line card will not be restarted or reloaded. This option applies only to ISSU upgrades between two software releases that have the same line card software. • WARM_RELOAD indicates that software was preloaded onto the line card, but the line card must be restarted with the new software. This option is equivalent to a soft reset of the line card. • RELOAD indicates that software was not preloaded onto the line card, which means that the line card will be reloaded. This option is equivalent to a hard reset of the line card. • INVALID indicates that you entered the show issu outage command outside the ISSU command sequence.
Max Outage Time	The length of time the line card will be unavailable after it is restarted.

Related Commands

Command	Description
issu loadversion	Starts the ISSU process.

show issu patch

To provide information about upgrade installation on both active and standby routers, use the **show issu patch** command in privileged EXEC mode.

show issu patch {pending {disk} | context | type {image | patch}}

Syntax Description

pending	Provides information about the impact of a pending upgrade.
<i>disk</i>	The disk on which the upgrade will occur.
context	Provides information about the installation and upgrade during the upgrade procedure.
type	Provides information about the patch or image to which the system is being upgraded.
image	Provides information about the image to which the system is being upgraded.
patch	Provides information about the upgrade.

Command Default

No information about the upgrade is displayed.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **show issu patch** command provides an overview of the impact on a system upgrade before and during the upgrade procedure.

Examples

The following example provides information about a pending upgrade on disk0:

```
Router# show issu patch pending disk0:/sys
```

```
Overall Impact of the pending upgrade:
```

```
Search Root: disk0:/sys
```

```
Type of upgrade: New base image
```

```
Action: Go Standby
```

Slot #	Card Type	Impacted
1	48 port 10/100 mb RJ-45 ethernet	Yes
2	SFM-capable 16 port 1000mb GBIC	Yes
3	48 port 10/100 mb RJ-45 ethernet	Yes
4	CEF720 48 port 10/100/1000mb Ethernet	Yes
8	CEF720 48 port 10/100/1000mb Ethernet	Yes
9	Intrusion Detection System	Yes

Table 15 describes significant fields shown in the display.

Table 15 *show issu patch Descriptions*

Field	Description
Overall Impact of the pending upgrade:	The command output shows the overall impact of an upgrade on a specified disk.
Search Root: disk0:/sys	Disk on which the upgrade will occur.
Type of upgrade: New base image	Type of upgrade. The upgrade could be a new image or a patch.
Action: Go Standby	Activates the upgrade on the standby router.
Slot #	Slot number on the router.
Card type	Type of card installed in the specified slot.
Impacted	States whether or not the card in the specified slot is affected by the upgrade.

show issu platform img-dnld

To display the progression of image download from slave to the Versatile Interface Processors (VIPs) and to display Minimal Disruptive Restart (MDR) details on Cisco 7600 series routers, use the **show issu platform img-dnld** command in user EXEC or privileged EXEC mode.

show issu platform img-dnld

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines The **show issu platform img-dnld** command is specific to Cisco 7600 series routers.

The **show issu platform img-dnld** command provides information to help you troubleshoot problems that may occur when performing an enhanced Fast Software Upgrade (eFSU). Entering this command allows you to display the progression of the image download from the slave unit to the VIPs and to display other details such as the following:

- Percentage completion of image downloads to the VIPs
- For each VIP in the router, the following is displayed:
 - The name of the VIP
 - Whether the slot is enabled
 - Whether a specified slot supports MDR
 - How much free memory is available if a slot is MDR-feasible
 - A message about image download if a slot supports MDR
- Information regarding whether single line card reload (SLCR) is enabled
- Number of MDR nonsupported slots
- Number of nonempty slots
- Number of line cards
- Number of MDR-feasible cards
- Number of MDR-incapable cards
- Number of MDR-capable cards
- MDR-ready cards

This command is available for eFSU on the Cisco 7600 series router platform only.

Examples

The following example output displays information before the download has been started:

```
Router# show issu platform img-dnld

Image download not performed yet.

Slot 1:  VIP2 R5K, Slot enabled, does not support MDR.
Slot 5:  VIP2 R5K, Slot enabled, does not support MDR.
Slot 9:  VIP6-80 RM7000B, Slot enabled, Supports MDR (205702684 bytes Free).  Image not
downloaded.

SLCR                               : enabled
MDR Unsupported slots              : 1  5
MDR Supported slots                : 9
No. of Non empty slots            : 5
No. of Line cards                  : 3
No. of MDR feasible cards         : 1
No. of MDR Incapable cards        : 2
No. of MDR capable cards          : 1 (0 LC(s) disabled)
MDR ready cards                    : 0
```

Table 16 describes the significant fields shown in the display.

Table 16 *show issu platform img-dnld Field Descriptions*

Field	Description
Slot 1: VIP2 R5K, Slot enabled, does not support MDR.	Slot 1, which holds a VIP2 R5K line card, does not support MDR.
Slot 5: VIP2 R5K, Slot enabled, does not support MDR.	Slot 5, which holds a VIP2 R5K line card, does not support MDR.
Slot 9: VIP6-80 RM7000B, Slot enabled, Supports MDR (205702684 bytes Free). Image not downloaded.	Slot 9, which holds a VIP6-80 RM7000B line card, supports MDR and has approximately 205 MB of free space.
SLCR : enabled	SLCR is enabled.
MDR Unsupported slots: 1 5	Slots holding line cards that are MDR-feasible but do not have enough memory in the VIP to download the image.
MDR Supported slots: 9	Slots holding line cards that are MDR-capable.
No. of Non empty slots: 5	Total number of nonlegacy cards, legacy cards, and Route Processors (RPs) in the router.
No. of Line cards : 3	Total number of nonlegacy line cards.

Table 16 *show issu platform img-dnld Field Descriptions (continued)*

Field	Description
No. of MDR feasible cards:1	Total number of nonlegacy line cards that are one of the following types: <ul style="list-style-type: none"> • VIP 4-50 controller • VIP 4-80 controller • VIP 6-80 controller • GEIP+ controller.
No. of MDR Incapable cards : 2	Total number of slots holding MDR unsupported line cards.
No. of MDR capable cards: 1 (0 LC(s) disabled)	Total number of line cards that are both MDR-feasible and have free memory to support at least image size plus 5 MB.
MDR ready cards: 0	Line cards in which the image has been downloaded.

The following sample output occurred during image download. The example shows that 25 percent of the image is downloaded to VIPs. Because slot 1 and slot 5 are not MDR supported, these two line cards will be reloaded during switchover.

```
Router# show issu platform img-dnld

Image downloading, 25% complete (1619968 / 6269374 bytes)

Slot 1: VIP2 R5K, Slot enabled, does not support MDR.
Slot 5: VIP2 R5K, Slot enabled, does not support MDR.
Slot 9: VIP6-80 RM7000B, Slot enabled, Supports MDR (190981516 bytes Free).
      Image is downloading
SLCR                               : enabled
MDR Unsupported slots              : 1  5
MDR Supported slots                : 9
No. of Non empty slots            : 5
No. of Line cards                  : 3
No. of MDR feasible cards         : 1
No. of MDR Incapable cards       : 2
No. of MDR capable cards         : 1 (0 LC(s) disabled)
MDR ready cards                    : 0
2 VIP(s) will be reloaded.
```

The following example output occurs after the image was downloaded. The examples shows that slot 9 completed the image download, and that the line card in slot 9 now has nearly 190 MB of free space:

```
Router# show issu platform img-dnld

Image download complete.

Slot 1: VIP2 R5K, Slot enabled, does not support MDR.
Slot 5: VIP2 R5K, Slot enabled, does not support MDR.
Slot 9: VIP6-80 RM7000B, Slot enabled, Supports MDR (190995548 bytes
Free). Image downloaded.

SLCR                               : enabled
MDR Unsupported slots              : 1  5
MDR Supported slots                : 9
No. of Non empty slots            : 5
No. of Line cards                  : 3
No. of MDR feasible cards         : 1
```

```

No. of MDR Incapable cards : 2
No. of MDR capable cards  : 1 (0 LC(s) disabled)
MDR ready cards           : 1
2 VIP(s) will be reloaded.

```

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.

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 (#)

Command History	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 17](#) describes the significant fields shown in the display.

Table 17 *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 issu sessions

To display detailed information about a particular In Service Software Upgrade (ISSU) client—including whether the client status for the impending software upgrade is compatible—use the **show issu sessions** command in user EXEC or privileged EXEC mode.

show issu sessions *client-id*

Syntax Description	<i>client-id</i>	The identification number used by ISSU for the client.
---------------------------	------------------	--

Command Modes	User EXEC (>) Privileged EXEC (#)
----------------------	--------------------------------------

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	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 you are not sure of the Client_ID number to enter into this command, use the show issu clients command to display the current list of clients with their names and ID numbers.
-------------------------	--

Examples The following example shows detailed information about the LDP Client:

```
Router# show issu sessions 2011

Client_ID = 2011, Entity_ID = 1 :

*** Session_ID = 46, Session_Name = LDP Session :

  Peer   Peer  Negotiate  Negotiated  Cap    Msg    Session
UniqueID Sid   Role       Result      GroupID GroupID Signature
  4      34   PRIMARY   COMPATIBLE  1      1      0
                               (no policy)

Negotiation Session Info for This Message Session:
  Nego_Session_ID = 46
  Nego_Session_Name = LDP Session
  Transport_Mtu = 3948
```

Table 18 describes the significant fields shown in the display.

Table 18 *show issu sessions Field Descriptions*

Field	Description
Client_ID	The identification number used by ISSU for that client.
Entity_ID	The identification number used by ISSU for each entity within this client.
Session_ID	The identification number used by ISSU for this session.
Session_Name	A character string describing the session.
Peer UniqueID	An identification number used by ISSU for a particular endpoint, such as a Route Processor or line card (could be a value based on slot number, for example). The peer that has the smaller unique_ID becomes the Primary (initiating) side in the capability and message version negotiations.
Peer Sid	Peer session ID.
Negotiate Role	Negotiation role of the endpoint: either PRIMARY (in which case the device initiates the negotiation) or PASSIVE (in which case the device responds to a negotiation initiated by the other device).
Negotiated Result	The features (“capabilities”) of this client’s new software were found to be either COMPATIBLE or INCOMPATIBLE with the intended upgrade process. (“Policy” means that an override of the negotiation result has been allowed by the software. Likewise, “no policy” means that no such override is present to be invoked).
Cap GroupID	Capability group ID: the identification number used for a list of distinct functionalities that the client application contains.
Msg GroupID	Message group ID: the identification number used for a list of formats employed when conveying information between the active device and the standby device.
Session Signature	Session signature: a unique ID to identify a current session in a shared negotiation scenario.
Nego_Session_ID	Negotiation session ID: the identification number used by ISSU for this negotiation session.
Nego_Session_Name	Negotiation session name: a character string describing this negotiation session.
Transport_Mtu	Maximum packet size (in bytes) of the ISSU messages conveyed between the two endpoints. A value of 0 means there is no restriction on size; in this case, fragmentation and reassembly then are handled in a manner transparent to the ISSU infrastructure.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications on this network supported by ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.

show issu state

To display the state and current version of the Route Processors (RPs) during the In Service Software Upgrade (ISSU) process, use the **show issu state** command in user EXEC or privileged EXEC mode.

show issu state [slot / port] [**detail**]

Syntax Description	
<i>slot</i>	(Optional) PRE slot number.
<i>port</i>	(Optional) PRE port number.
detail	(Optional) Provides detailed information about the state of the active and standby RPs.

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

Command History	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)SRB1.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	12.2(33)SCD2	This command was implemented on the Cisco CMTS routers in Cisco IOS Release 12.2(33)SCD2.

Usage Guidelines	
	Use the show issu state command to display the state and current version of each RP.
	It may take several seconds after the issu loadversion command is entered for Cisco IOS software to load onto the standby RP and the standby RP to transition to stateful switchover (SSO) mode. If you enter the show issu state command too soon, you may not see the information you need.

Examples	
	The following example displays the manner in which the ISSU state is verified.

```
Router# show issu state detail

          Slot = A
          RP State = Active
          ISSU State = Init
          Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
          Operating Mode = SSO
          Primary Version = N/A
          Secondary Version = N/A
```

```

Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
Variable Store = PrstVbl

Slot = B
RP State = Standby
ISSU State = Init
Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
Operating Mode = SSO
Primary Version = N/A
Secondary Version = N/A
Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
    
```

```

Slot Red Role Peer Act/Sby Image Match RP LC ISSU State ISSU Proc
-----
5/0 Secondary - standby Yes - -
6/0 Primary 5/0 active Yes - -
7/0 Primary 5/0 active Yes - -
8/0 Primary 5/0 active Yes - -
PRE is the new active: FALSE
Waiting for MDR: FALSE
No Transitional Line Card State information registered.
No Peer Line Card State information registered.
Peer Line Card Action:
-----Card Type----- Action----- Slots-----
24rfchannel-spa-1 NO ACTION 0x00000004
4jacket-1 NO ACTION 0x00000004
2cable-dtcc NO ACTION 0x00000028
1gigethereth-hh-1 NO ACTION 0x00000200
    
```

Table 19 describes the significant fields shown in the display.



Note

Fields that are described after the *Slot* field under the “Standby RP” section in the table refer to the line card ISSU status.

Table 19 show issu state Field Descriptions

Field	Description
Active RP	
Slot = A	The RP slot that is being used.
RP State = Active	State of this RP.
ISSU State = Init	The in service software upgrade (ISSU) process is in its initial state.
Boot Variable = N/A	The RP’s boot variable.
Operating Mode = SSO	The RP’s operating mode.
Primary Version = N/A	The primary software image running on the RP.
Secondary Version = N/A	The secondary software image running on the RP.
Current Version = disk0:c10k2-p11-mz.1.20040830	The current software image running on the RP.
Standby RP	
Slot = B	The slot/subslot number pair for line card.
RP State = Standby	State of this RP.

Table 19 *show issu state Field Descriptions (continued)*

Field	Description
Slot	The slot number of the line card.
Red Role	Redundancy role of the line card.
Peer	The slot/ subslot pair of the protect line card.
Act/ Sby	The line card's current redundancy status.
Image Match RP	Indicates if the line card image matches the image of the current active RP.
LC ISSU State	The current line card ISSU state.
ISSU Proc	Indicates the progress of the current ISSU state.

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 changeversion	Performs a single-step complete ISSU upgrade process cycle.
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 of the active to the standby processor and causes the newly active processor to run the new image.

show mdr download image

To display the amount of memory needed to store the new software image on line cards that support enhanced Fast Software Upgrade (eFSU), use the **show mdr download image** command from the switch processor (SP) console in privileged EXEC mode.

show mdr download image

Syntax Description This command has no arguments or keywords.

Command Modes SP console

Command History	Release	Modification
	12.2(33)SRB1	This command was introduced on Cisco 7600 series routers.

Usage Guidelines You must issue the **show mdr download image** command from the SP console. You cannot issue the command from the line card or from the route processor (RP) console.

During an in service software upgrade (ISSU), the router preloads line card software onto line cards that support eFSU. As part of the software preload, the router automatically reserves memory on the line card to store the new software image (decompressed format).

You can use the **show mdr download image** command to determine how much memory is needed on the line cards for the new software image.



Note

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

Examples The following example shows how much memory will be reserved for the new software on the installed line cards:

```
Router# remote command switch show mdr download image
```

```
Pre-download information
Slot CPU In-Progress Complete LC Mem Resv (bytes)
1 0 N N 0
1 1 N N 0
2 0 N N 31719424
2 1 N N 0
3 0 N N 35913728
3 1 N N 0
4 0 N N 31719424
4 1 N N 0
5 0 N N 0
5 1 N N 0
6 0 N N 0
6 1 N N 0
7 0 N N 0
```

```

7    1    N      N      0
8    0    N      N      0
8    1    N      N      0
9    0    N      N      0
9    1    N      N      0
10   0    N      N      0
10   1    N      N      0
11   0    N      N      0
11   1    N      N      0
12   0    N      N      0
12   1    N      N      0
13   0    N      N      0
13   1    N      N      0

```

Router#

[Table 5](#) describes the fields in the display.

Table 20 *show mdr download image Field Descriptions*

Field	Description
Slot	The chassis slot number in which the line card is installed.
CPU	The CPU number on the line card.
In Progress	Indicates whether the software preload is active.
Complete	Indicates whether the software preload is finished.
LC Memory Reserve	The amount of memory (in bytes) that must be available on the line card to store the new line card software.

show monitor event-trace sbc

To display event trace messages for the Session Border Controller (SBC), use the **show monitor event-trace sbc** command in privileged EXEC mode.

```
show monitor event-trace sbc ha {all [detail] | back {minutes | hours:minutes} [detail] | clock
hours:minutes [day month] [detail] | from-boot [seconds] [detail] | latest [detail] |
parameters} 1
```

Syntax Description

ha	Displays event trace messages for SBC high availability (HA).
all	Displays all event trace messages currently in memory for SBC HA.
detail	(Optional) Displays detailed trace information.
back	Specifies how far back from the current time you want to view messages. For example, you can display messages from the last 30 minutes.
<i>minutes</i>	Time argument in minutes. The time argument is specified in minutes format (mmm).
<i>hours:minutes</i>	Time argument in hours and minutes. The time argument is specified in hours and minutes format (hh:mm).
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
<i>day month</i>	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting.
<i>seconds</i>	(Optional) Specified number of seconds to display event trace messages after booting. Range: 0 to the number of seconds elapsed since the boot.
latest	Displays only the event trace messages since the last show monitor event-trace sbc ha command was entered.
parameters	Displays the trace parameters. The parameters displayed are the size (number of trace messages) of the trace file and whether stacktrace is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.3	The sbc_ha keyword was changed to two keywords, sbc and ha .

Usage Guidelines

Use the **show monitor event-trace sbc ha** command to display trace message information for SBC HA. The trace function is not locked while information is displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace sbc ha** command generates a

message indicating that some messages might be lost; however, messages continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace sbc ha** command stops displaying messages.

Examples

The following is sample output from the **show monitor event-trace sbc ha all** command. In the following example, all messages from SBC HA events are displayed.

```
Router# show monitor event-trace sbc ha all

*Jan 16 07:21:49.718: RF: Is Active, from boot = 0x1
*Jan 16 07:21:49.720: IPC: Initialised as master
*Jan 16 07:21:49.720: RF: Active reached, from boot = 0x1
*Jan 16 07:21:59.448: ILT: Registered on 48, result = 0x1
*Jan 16 07:21:59.448: RF: Start SM on 48
*Jan 16 07:49:02.523: IPC: Session to peer opened
*Jan 16 07:49:02.605: ISSU: Negotiation starting
*Jan 16 07:49:02.605: RF: Delaying progression at 300
*Jan 16 07:49:02.617: ISSU: Negotiation done
*Jan 16 07:49:02.617: RF: Negotiation result = 0x1
*Jan 16 07:49:02.617: RF: Peer state change, peer state = 0x1
*Jan 16 07:49:02.617: RF: Resuming progression at event 300
*Jan 16 07:50:00.853: ISSU: Transformed transmit message
*Jan 16 07:50:00.853: IPC: Queuing message type SBC_HA_MPF_CAPS_MSG_TYPE
*Jan 16 07:50:00.854: IPC: Queued message type SBC_HA_MPF_CAPS_MSG_TYPE
```

Table 21 describes the significant fields shown in the display.

Table 21 *show monitor event-trace sbc ha all Field Descriptions*

Field	Description
RF:	Redundancy Facility (RF) events. RF controls and drives HA redundancy events.
IPC:	Interprocess communication (IPC) messages.
ILT:	Interlocation Transport (ILT) events. ILT is the interface and mechanism for transporting SBC HA data.
ISSU:	In Service Software Upgrade (ISSU) events.

The following is sample output from the **show monitor event-trace sbc ha latest** command. This command displays messages from SBC HA events since the last **show monitor event-trace sbc ha** command was entered.

```
Router# show monitor event-trace sbc ha latest

*Jan 16 07:50:00.922: IPC: Sent message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: IPC: Received message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: ISSU: Transformed received message
*Jan 16 07:50:00.922: ILT: Received IPS for PID 0x30105000, type = 0x16820002
*Jan 16 07:50:00.922: ILT: Target 49 is remote, for PID 0x31105000
*Jan 16 07:50:00.922: ILT: Send IPS to PID 0x31105000, type = 0x16820001
*Jan 16 07:50:00.922: ISSU: Transformed transmit message
*Jan 16 07:50:00.922: IPC: Queuing message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: IPC: Queued message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: IPC: Sent message type SBC_HA_SEND_IPS_MSG_TYPE
```

This command displays the messages since the last **show monitor event-trace sbc ha** command was entered.

Table 22 describes the significant fields shown in the display.

Table 22 *show monitor event-trace sbc ha latest Field Descriptions*

Field	Description
IPC:	IPC messages.
ILT:	ILT events. ILT is the interface and mechanism for transporting SBC HA data.
ISSU:	ISSU events.

The following is sample output from the **show monitor event-trace sbc ha parameters** command . This command displays the number of event-trace messages in the trace file and whether stacktrace is disabled.

```
Router# show monitor event-trace sbc ha parameters
```

```
Trace has 2048 entries
Stacktrace is disabled by default
```

Related Commands

Command	Description
monitor event-trace sbc (EXEC)	Monitors and controls the event trace function for the SBC.
monitor event-trace sbc (global)	Configures event tracing for the SBC.

show mpls ip iprm counters

To display the number of occurrences of various Multiprotocol Label Switching (MPLS) IP Rewrite Manager (IPRM) events, use the **show mpls ip iprm counters** command in privileged EXEC mode.

show mpls ip iprm counters

Syntax Description This command has no arguments or keywords.

Defaults No default behaviors or values.

Command Modes Privileged EXEC

Command History

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 routers.
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.

Usage Guidelines This command reports the occurrences of IPRM events.

Examples

The command in the following example displays the events that the IPRM logs:

```
Router# show mpls ip iprm counters

CEF Tree Changes Processed/Ignored:          91/12
CEF Deletes Processed/Ignored:              12/2
Label Discoveries:                           74
Rewrite Create Successes/Failures:          60/0
Rewrite Gets/Deletes:                       82/0
Label Announcements: Info/Local/Path:       6/119/80
Walks: Recursion Tree/CEF Full/CEF interface: 78/2/0
```

Table 23 describes the significant fields shown in the display.

Table 23 *show mpls ip iprm counters Command Field Descriptions*

Field	Description
CEF Tree Changes Processed/Ignored	<p>Processed—The number of Cisco Express Forwarding tree change announcements that IPRM processed.</p> <p>Ignored—The number of Cisco Express Forwarding tree change announcements that IPRM ignored.</p> <p>Typically, IPRM processes tree change announcements only for prefixes in a routing table.</p>
CEF Deletes Processed/Ignored	<p>Processed—The number of Cisco Express Forwarding delete entry announcements that IPRM processed.</p> <p>Ignored—The number of Cisco Express Forwarding delete entry announcements that IPRM ignored.</p> <p>Typically, IPRM processes delete entry announcements only for prefixes in a routing table.</p>
Label Discoveries	The number of label discoveries performed by IPRM. Label discovery is the process by which IPRM obtains prefix labels from the IP Label Distribution Modules (LDMs).
Rewrite Create Successes/Failures	<p>Successes—The number of times IPRM successfully updated the MPLS forwarding information.</p> <p>Failures—The number of times IPRM attempted to update the MPLS forwarding information and failed.</p>
Rewrite Gets/Deletes	<p>Gets—The number of times IPRM retrieved forwarding information from the MPLS forwarding infrastructure.</p> <p>Deletes—The number of times IPRM removed prefix forwarding information from the MPLS forwarding infrastructure.</p>

Table 23 *show mpls ip iprm counters Command Field Descriptions (continued)*

Field	Description
CEF Tree Changes Processed/Ignored	<p>Processed—The number of Cisco Express Forwarding tree change announcements that IPRM processed.</p> <p>Ignored—The number of Cisco Express Forwarding tree change announcements that IPRM ignored.</p> <p>Typically, IPRM processes tree change announcements only for prefixes in a routing table.</p>
Label Announcements: Info/Local/Path	<p>Info—The number of times an IP label distribution module informed IPRM that label information for a prefix changed.</p> <p>Local—The number of times an IP label distribution module specified local labels for a prefix.</p> <p>Path—The number of times an IP LDM specified outgoing labels for a prefix route.</p>
Walks: Recursion Tree/CEF Full/CEF interface	<p>Recursion Tree—The number of times IPRM requested Cisco Express Forwarding to walk the recursion (path) tree for a prefix.</p> <p>CEF Full—The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix.</p> <p>CEF interface—The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix with a path that uses a specific interface.</p>

Related Commands

Command	Description
clear mpls ip iprm counters	Clears the IPRM counters.
show mpls ip iprm ldm	Displays information about the IP LDMs that have registered with the IPRM.

show mpls ip iprm ldm

To display information about the IP Label Distribution Modules (LDMs) that have registered with the IP Rewrite Manager (IPRM), use the **show mpls ip iprm ldm** command in privileged EXEC mode.

```
show mpls ip iprm ldm [table {all | table-id} | vrf vrf-name] [ipv4 | ipv6]
```

Cisco 10000 Series Routers

```
show mpls ip iprm ldm [table {all | table-id} | vrf vrf-name] [ipv4]
```

Syntax Description

table	(Optional) Displays the LDMs for one or more routing tables.
all	Displays the LDMs for all routing tables.
<i>table-id</i>	Displays the LDMs for the routing table you specify. Table 0 is the default or global routing table.
vrf	(Optional) Displays the LDMs for the VPN routing and forwarding (VRF) instance you specify.
<i>vrf-name</i>	(Optional) The name of the VRF instance. You can find VRF names with the show ip vrf command.
ipv4	(Optional) Displays IPv4 LDMs.
ipv6	(Optional) Displays IPv6 LDMs.
	Note Applies to Cisco 7500 series routers only.

Defaults

If you do not specify any keywords or parameters, the command displays the LDMs for the global routing table (the default).

Command Modes

Privileged EXEC

Command History

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 routers.
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)SSH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the IP LDMs registered with IPRM.

Examples

The command in the following example displays the LDMs for the global routing tables. It shows that two LDMs (lcatm and ldp) are registered for the ipv4 global routing table, and that one LDM (bgp ipv6) is registered for the ipv6 global routing table.

```
Router# show mpls ip iprm ldm

table (global;ipv4); ldms: 2
  lcatm, ldp
table (global;ipv6); ldms: 1
  bgp ipv6
```

The command in the following example displays all of the LDMs registered with IPRM. The output shows the following:

- The LDMs called lcatm and ldp have registered with IPRM for the ipv4 global table.
- The LDM called bgp ipv6 is registered for the IPv6 global table.
- The LDM called bgp vpv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all

table (global;ipv4); ldms: 2
  lcatm, ldp
table (global;ipv6); ldms: 1
  bgp ipv6
table (all-tbls;ipv4); ldms: 1
  bgp vpv4
```

The command in the following example displays the LDMs registered for the IPv6 routing tables.

```
Router# show mpls ip iprm ldm ipv6

table (global;ipv6); ldms: 1
  bgp ipv6
```

Cisco 10000 Series Examples Only

The command in the following example displays the LDMs for the global routing tables. It shows that one LDM (ldp) is registered for the ipv4 global routing table.

```
Router# show mpls ip iprm ldm

table (global;ipv4); ldms: 1
  ldp
```

The command in the following example displays all of the LDMs registered with IPRM. The output shows the following:

- The LDM called ldp has registered with IPRM for the ipv4 global table.
- The LDM called bgp vpv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all

table (global;ipv4); ldms: 1
  ldp
table (all-tbls;ipv4); ldms: 1
  bgp vpv4
```

Related Commands

Command	Description
show mpls ip iprm counters	Displays the number of occurrences of various IPRM events.

show platform redundancy bias

To display output for a specific standby slot SUP bootup delay setting, use the **show platform redundancy bias** command in privileged EXEC mode.

show platform redundancy bias

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SRD4	This command was introduced on the Cisco 7600 Series Routers.

Usage Guidelines Use the **show platform redundancy bias** command to display the output for a specific **platform redundancy bias** command.

Examples The following example shows how to verify the standby slot SUP bootup delay setting after configuring it for 50 seconds:

```
Router# configure terminal
Router(config)# platform redundancy bias 50
Router(config)# end
Router#show platform redundancy bias
Platform redundancy bias is set at 50 seconds
```



Note Using the **show platform redundancy bias** without configuring a value for the delay displays an error message.

Related Commands	Command	Description
	platform redundancy bias	Configures the standby slot SUP bootup delay setting.

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 (#)

Command History

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.

Release	Modification
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.
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 Clie(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

```

Cisco AS5850 Example

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

```

Cisco AS5800 Example

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.

```

Cisco AS5800 with History Example

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
```

Cisco AS5800 Router Shelves as Failover Pair Example

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.

Log from the First Router (RouterA)

```
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
```

Log from the Second Router (RouterB)

```
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
```

Privileged EXEC Mode Example

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 mode	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.

show tcp ha connections

To display connection-ID-to-TCP mapping data, use the **show tcp ha connections** command in privileged EXEC mode.

show tcp ha connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show tcp ha connections** command is used to display connection-ID-to-TCP mapping data.

Examples

The following is sample output from the **show tcp ha connections** command:

```
Router# show tcp ha connections
```

```
SSO enabled for 40 connections
TCB      Local Address      Foreign Address      (state)    Conn Id
71EACE60 10.0.56.1.179      10.0.56.3.58671     ESTAB      37
71EA9320 10.0.53.1.179      10.0.53.3.58659     ESTAB      34
71EA35F8 10.0.41.1.179      10.0.41.3.58650     ESTAB      22
71A21FE0 10.0.39.1.179      10.0.39.3.58641     ESTAB      20
71EAA6E0 10.0.54.1.179      10.0.54.3.58663     ESTAB      35
71EA2238 10.0.40.1.179      10.0.40.3.58646     ESTAB      21
71EABAA0 10.0.55.1.179      10.0.55.3.58667     ESTAB      36
71EAE710 10.0.28.1.179      10.0.28.3.58676     ESTAB      9
71EA2728 10.0.50.1.179      10.0.50.3.58647     ESTAB      31
720541D8 10.0.49.1.179      10.0.49.3.58642     ESTAB      30
71EAA1F0 10.0.44.1.179      10.0.44.3.58662     ESTAB      25
2180B3A8 10.0.33.1.179      10.0.33.3.58657     ESTAB      14
71EAB5B0 10.0.45.1.179      10.0.45.3.58666     ESTAB      26
21809FE8 10.0.32.1.179      10.0.32.3.58653     ESTAB      13
71EA8E30 10.0.43.1.179      10.0.43.3.58658     ESTAB      24
71EAD350 10.0.27.1.179      10.0.27.3.58672     ESTAB      8
2180A9C8 10.0.52.1.179      10.0.52.3.58655     ESTAB      33
2180A4D8 10.0.42.1.179      10.0.42.3.58654     ESTAB      23
71EABF90 10.0.26.1.179      10.0.26.3.58668     ESTAB      7
71EA3AE8 10.0.51.1.179      10.0.51.3.58651     ESTAB      32
720546C8 10.0.59.1.179      10.0.59.3.58643     ESTAB      40
```

Table 24 describes the significant fields shown in the display.

Table 24 *show tcp ha connections Field Descriptions*

Field	Description
SSO enabled for	Displays the number of TCP connections that support BGP Nonstop Routing (NSR) with SSO.
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	<p>TCP connection state. A connection progresses through a series of states during its lifetime. The states that follow are shown in the order in which a connection progresses through them.</p> <ul style="list-style-type: none"> • LISTEN—Waiting for a connection request from any remote TCP and port. • SYNSENT—Waiting for a matching connection request after having sent a connection request. • SYNRCVD—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB—Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1—Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent.
Conn id	Identifying number of the TCP connection.

site-id

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

site-id *alphanumeric*

no site-id *alphanumeric*

Syntax Description	<i>alphanumeric</i>	Site identifier, using up to 200 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).
---------------------------	---------------------	---

Command Default	No site 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 site-id command is optional.
-------------------------	---

Examples	The following example configures “Site1ManhattanNY” as the customer ID without spaces:
-----------------	--

```
Router(config)# call-home
Router(cfg-call-home)# site-id Site1ManhattanNY
```

The following example configures “Site1 Manhattan NY” as the customer ID using spaces and required “ ” notation:

```
Router(config)# call-home
Router(cfg-call-home)# site-id "Site1 Manhattan NY"
```

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.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [**vrrp**]

no snmp-server enable traps [*notification-type*] [**vrrp**]

Syntax Description

notification-type

(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the **no** form is used). The notification type can be one of the following keywords:

alarms—Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values.

- The *severity* argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4 (informational). Severity levels are defined as follows:
 - 1—Critical. The condition affects service.
 - 2—Major. Immediate action is needed.
 - 3—Minor. Minor warning conditions.
 - 4—Informational. No action is required. This is the default.
- **auth-framework** [**sec-violation**]—Enables the SNMP CISCO-AUTH-FRAMEWORK-MIB traps. The optional **sec-violation** keyword enables the SNMP camSecurityViolationNotif notification.¹
- **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent.
- **dot1x**—Enables IEEE 802.1X traps. This notification type is defined in the CISCO PAE MIB.

Catalyst 6500 Series Switches

The following keywords are available under the **dot1x** keyword:

- **auth-fail-vlan**—Enables the SNMP cpaeAuthFailVlanNotif notification.
- **no-auth-fail-vlan**—Enables the SNMP cpaeNoAuthFailVlanNotif notification.
- **guest-vlan**—Enables the SNMP cpaeGuestVlanNotif notification.
- **no-guest-vlan**—Enables the SNMP cpaeNoGuestVlanNotif notification.

- **ds0-busyout**—Sends notification when the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2), and the notification type is (1) cpmDS0BusyoutNotification.
- **ds1-loopback**—Sends notification when the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as (2) cpmDS1LoopbackNotification.
- **dsp**—Enables SNMP digital signal processing (DSP) traps. This notification type is defined in the CISCO-DSP-MGMT-MIB.
- **dsp oper-state**—Sends a DSP notification made up of both a DSP ID that indicates which DSP is affected and an operational state that indicates whether the DSP has failed or recovered.
- **l2tc**—Enable the SNMP Layer 2 tunnel configuration traps. This notification type is defined in CISCO-L2-TUNNEL-CONFIG-MIB.¹
- **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as (1) entConfigChange.
- **entity-diag type**— Enables the SNMP CISCO-ENTITY-DIAG-MIB traps. The valid *type* values are as follows:¹
 - **boot-up-fail**—(Optional) Enables the SNMP ceDiagBootUpFailedNotif traps.¹
 - **hm-test-recover**—(Optional) Enables the SNMP ceDiagHMTTestRecoverNotif traps.¹
 - **hm-thresh-reached**—(Optional) Enables the SNMP ceDiagHMThresholdReachedNotif traps.¹
 - **scheduled-fail**—(Optional) Enables the SNMP ceDiagScheduledJobFailedNotif traps.¹
- **flowmon**—Controls flow monitoring notifications.
- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is (1) cHsrpStateChange.
- **ipmulticast**—Controls IP multicast notifications.
- **license**—Enables licensing notifications as traps or informs. The notifications are grouped into categories that can be individually controlled by combining the keywords with the **license** keyword, or as a group by using the **license** keyword by itself.
 - **deploy**—Controls notifications generated as a result of install, clear, or revoke license events.
 - **error**—Controls notifications generated as a result of a problem with the license or with the usage of the license.
 - **imagelevel**—Controls notifications related to the image level of the license.
 - **usage**—Controls usage notifications related to the license.
- **modem-health**—Controls modem-health notifications.

- **module-auto-shutdown [status]**—Enables the SNMP CISCO-MODULE-AUTO-SHUTDOWN-MIB traps. The optional **status** keyword enables the SNMP Module Auto Shutdown status change traps.¹
- **rsvp**—Controls Resource Reservation Protocol (RSVP) flow change notifications.
- **sys-threshold**—(Optional) Enables the SNMP cltcTunnelSysDropThresholdExceeded notification. This notification type is an enhancement to the CISCO-L2-TUNNEL-CONFIG-MIB.¹
- **tty**—Controls TCP connection notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my, and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification.

Note For additional notification types, see the Related Commands table.

vrrp (Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).

1. Supported on the Catalyst 6500 series switches.

Command Default No notifications controlled by this command are sent.

Command Modes Global configuration (config)

Command History	Release	Modification
	10.3	This command was introduced.
	12.0(2)T	The rsvp notification type was added in Cisco IOS Release 12.0(2)T.
	12.0(3)T	The hsrp notification type was added in Cisco IOS Release 12.0(3)T.
	12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
	12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
	12.3(11)T	The vrrp notification type was added in Cisco IOS Release 12.3(11)T.
	12.4(4)T	Support for the alarms notification type and <i>severity</i> argument was added in Cisco IOS Release 12.4(4)T. Support for the dsp and dsp oper-state notification types was added in Cisco IOS Release 12.4(4)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.
	12.4(11)T	The dot1x notification type was added in Cisco IOS Release 12.4(11)T.
	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.

Release	Modification
12.4(20)T	The license notification type keyword was added.
12.2(33)SXH	The l2tc keyword was added and supported on the Catalyst 6500 series switch.
12.2(33)SXI	The following keywords were added and supported on the Catalyst 6500 series switch: <ul style="list-style-type: none"> • auth-fail-vlan • entity-diag • guest-vlan • module-auto-shutdown • no-auth-fail-vlan • no-guest-vlan • sys-threshold
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	The flowmon notification type was added in Cisco IOS Release 15.0(1)S.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host [traps | informs]** command.

To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

Most notification types are disabled by default but some cannot be controlled with the **snmp-server enable traps** command.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

Catalyst 6500 Series Switches

The following MIBs were enhanced or supported in Cisco IOS Release 12.2(33)SXI and later releases on the Catalyst 6500 series switch:

- CISCO-L2-TUNNEL-CONFIG-MIB-LLDP—Enhancement. The CISCO-L2-TUNNEL-CONFIG-MIB provides SNMP access to the Layer 2 tunneling-related configurations.
- CISCO-PAE-MIB—Enhancement for critical condition and includes traps when the port goes into the Guest Vlan or AuthFail VLAN.
- CISCO-MODULE-AUTO-SHUTDOWN-MIB—Supported. The CISCO-MODULE-AUTO-SHUTDOWN-MIB provides SNMP access to the Catalyst 6500 series switch Module Automatic Shutdown component.

- CISCO-AUTH-FRAMEWORK-MIB—Supported. The CISCO-AUTH-FRAMEWORK-MIB provides SNMP access to the Authentication Manager component.
- CISCO-ENTITY-DIAG-MIB—The CISCO-ENTITY-DIAG-MIB provides SNMP traps for generic online diagnostics (GOLD) notification enhancements.

Examples

The following example shows how to enable the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example shows how to configure an alarm severity threshold of 3:

```
Router# snmp-server enable traps alarms 3
```

The following example shows how to enable the generation of a DSP operational state notification from the command-line interface (CLI):

```
Router(config)# snmp-server enable traps dsp oper-state
```

The following example shows how to enable the generation of a DSP operational state notification from a network management device:

```
setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1
cdspEnableOperStateNotification.0=true(1)
```

The following example shows how to send no traps to any host. The Border Gateway Protocol (BGP) traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host user1 public isdn
```

The following example shows how to enable the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The following example shows that VRRP will be used as the protocol to enable the traps:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c vrrp
```

The following example shows how to send IEEE 802.1X MIB traps to the host “myhost.example.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps dot1x
Router(config)# snmp-server host myhost.example.com traps public
```

Related Commands	Command	Description
	snmp-server enable traps atm pvc	Enables ATM PVC SNMP notifications.
	snmp-server enable traps atm pvc extension	Enables extended ATM PVC SNMP notifications.
	snmp-server enable traps bgp	Enables BGP server state change SNMP notifications.
	snmp-server enable traps calltracker	Enables Call Tracker callSetup and callTerminate SNMP notifications.
	snmp-server enable traps envmon	Enables environmental monitor SNMP notifications.
	snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status change SNMP notifications.
	snmp-server enable traps ipsec	Enables IPsec SNMP notifications.
	snmp-server enable traps isakmp	Enables IPsec ISAKMP SNMP notifications.
	snmp-server enable traps isdn	Enables ISDN SNMP notifications.
	snmp-server enable traps memory	Enables memory pool and buffer pool SNMP notifications.
	snmp-server enable traps mpls ldp	Enables MPLS LDP SNMP notifications.
	snmp-server enable traps mpls traffic-eng	Enables MPLS TE tunnel state-change SNMP notifications.
	snmp-server enable traps mpls vpn	Enables MPLS VPN specific SNMP notifications.
	snmp-server enable traps repeater	Enables RFC 1516 hub notifications.
	snmp-server enable traps snmp	Enables RFC 1157 SNMP notifications.
	snmp-server enable traps syslog	Enables the sending of system logging messages via SNMP.
	snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
	snmp-server informs	Specifies inform request options.
	snmp-server trap-source	Specifies the interface (and the corresponding IP address) from which an SNMP trap should originate.
	snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.
	vrrp shutdown	Disables a VRRP group.

street-address

To specify a street address where RMA equipment for Call Home can be sent, use the **street-address** command in call home configuration mode. To remove the street address, use the **no** form of this command.

street-address *alphanumeric*

no street-address *alphanumeric*

Syntax Description	<i>alphanumeric</i>	Street address, using up to 200 alphanumeric characters, including commas and spaces. If you include spaces, you must enclose your entry in quotes (“ ”).
---------------------------	---------------------	---

Command Default No street address is specified.

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 **street-address** command is optional to specify where return materials authorization (RMA) equipment for Call Home should be sent.

Examples The following example configures “1234AnyStreet,AnyCity,AnyState,12345” as the street address without spaces:

```
Router(config)# call-home
Router(cfg-call-home)# street-address 1234AnyStreet,AnyCity,AnyState,12345
```

The following example configures “1234 Any Street, Any City, Any State, 12345” as the street address using commas and spaces with required “ ” notation:

```
Router(config)# call-home
Router(cfg-call-home)# street-address "1234 Any Street, Any City, Any State, 12345"
```

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.

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. <ul style="list-style-type: none"> <i>sessions</i>—Range 1 to 32000, default is 250. <i>seconds</i>—Range is 1 to 33550, default is 1.

Command Default

Subscriber redundancy policy applies default values.

Command Modes

Global configuration

Command History

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.

subscribe-to-alert-group

To subscribe a destination profile to an alert group, use the **subscribe-to-alert-group** command in destination profile configuration mode. To unsubscribe from an alert group or all alert groups, use the **no** form of this command.

subscribe-to-alert-group { **all** | **configuration** [**periodic** { **daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm* }] | **diagnostic** [**severity** *level*] | **environment** | **inventory** | **syslog** }

Syntax Description

all	Subscribes to all alert groups.
configuration	Subscribes to configuration information groups.
periodic daily <i>hh:mm</i>	(Optional) Specifies the time to begin daily Call Home messages. The valid values for the time are based on a 24-hour clock.
periodic monthly <i>day hh:mm</i>	(Optional) Specifies the time to begin monthly Call Home messages; the valid values are as follows: <ul style="list-style-type: none"> • <i>day</i> is 1 to 31. • <i>hh:mm</i> is based on a 24-hour clock.
periodic weekly <i>day hh:mm</i>	(Optional) Specifies the time to begin weekly Call Home messages; the valid values are as follows: <ul style="list-style-type: none"> • <i>day</i> is 1 to 31. • <i>hh:mm</i> is based on a 24-hour clock.
diagnostic	Subscribes to diagnostic information groups.
severity <i>level</i>	Specifies the severity level of the diagnostic.
environment	Subscribes to environmental information groups.
inventory	Subscribes to inventory information groups.
syslog	Subscribes to system logging (syslog) information groups.

Command Default

Destination profiles are not subscribed to alert groups by default.

Command Modes

Destination profile configuration

Command History

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

Usage Guidelines

The valid values for the *level* argument are as follows:

- **catastrophic**—Catastrophic event
- **critical**—Critical event
- **debugging**—Debugging event
- **disaster**—Disaster event

- **fatal**—Fatal event
- **major**—Major event
- **minor**—Minor event
- **normal**—Normal event
- **notification**—Notification event
- **warning**—Warning event

Selecting the lowest severity level includes all higher severity events. The types of severity levels are as follows:

- Catastrophic—A network-wide catastrophic failure (Highest severity)
- Disaster—A significant network impact
- Fatal—System is unusable (System log level 0)
- Critical—Immediate attention needed (System log level 1)
- Major—Major condition (System log level 2)
- Minor—Minor condition (System log level 3)
- Warning—Warning condition (System log level 4)
- Notification—Informational message (System log level 5)
- Normal—Signifying returning to normal state (System log level 6)
- Debug—Debugging message (Lowest severity)

Examples

The following examples shows how to subscribe to all alert groups:

```
subscribe-to-alert-group all
```

subscribe-to-alert-group all

To configure a destination profile to receive messages for all available alert groups for Call Home, use the **subscribe-to-alert-group all** command in call home profile configuration mode. To remove the subscription, use the **no** form of this command.

subscribe-to-alert-group all

no subscribe-to-alert-group all

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

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

To enter call home profile configuration mode, use the **profile (call home)** command in call home configuration mode.



Note

Alert group trigger events and the commands that are executed because of a trigger are platform-dependent. For more information, see the corresponding Call Home configuration documentation for your platform.



Caution

The **subscribe-to-alert-group all** command subscribes you to all debug-level syslog messages. The number of messages produced can overload the system.

Examples

The following example shows how to configure a profile to receive messages for all available alert groups:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile example
Switch(cfg-call-home-profile)# subscribe-to-alert-group all
```

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.
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 for the Syslog alert group for Call Home.

subscribe-to-alert-group configuration

To configure a destination profile to receive messages for the Configuration alert group for Call Home, use the **subscribe-to-alert-group configuration** command in call home profile configuration mode. To remove the subscription, use the **no** form of this command.

subscribe-to-alert-group configuration [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]

no subscribe-to-alert-group configuration [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]

Syntax Description	<p>periodic (Optional) Specifies a periodic Call Home message, where:</p> <ul style="list-style-type: none"> • daily <i>hh:mm</i>—Time [in 24-hour format (<i>hh:mm</i>)] for a daily Call Home alert notification to be sent. • monthly <i>day hh:mm</i>—Numeric day of the month (from 1 to 31) and time [in 24-hour format (<i>hh:mm</i>)] for a monthly Call Home alert notification to be sent. • weekly <i>day hh:mm</i>—Day of the week (Monday through Saturday) and time [in 24-hour format (<i>hh:mm</i>)] for a weekly Call Home alert notification to be sent.
---------------------------	---

Command Default	This command has no default behavior or values.
------------------------	---

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	<p>To enter call home profile configuration mode, use the profile (call home) command in call home configuration mode.</p> <p>When you subscribe to the Configuration alert group without the periodic option, a notification occurs whenever a configuration change occurs. Otherwise, the notification occurs at the date and time specified.</p>
-------------------------	---

**Note**

Alert group trigger events and the commands that are executed because of a trigger are platform-dependent. For more information, see the corresponding Call Home configuration documentation for your platform.

Examples

The following example shows how to configure a profile to receive a weekly periodic configuration alert notification every Tuesday at 9:16 PM (21:16):

```
Switch(config)# call-home
Switch(cfg-call-home)# profile example
Switch(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Tuesday 21:16
```

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.
subscribe-to-alert-group all	Configures a destination profile to receive messages for all available alert groups 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.

subscribe-to-alert-group diagnostic

To configure a destination profile to receive messages for the Diagnostic alert group for Call Home, use the **subscribe-to-alert-group diagnostic** command in call home profile configuration mode. To remove the subscription, use the **no** form of this command.

subscribe-to-alert-group diagnostic [**severity** { **catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning** }]

no subscribe-to-alert-group diagnostic [**severity** { **catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning** }]

Syntax Description

severity	<p>(Optional) Specifies the lowest level of severity events to include in a diagnostic alert, where:</p> <ul style="list-style-type: none"> • catastrophic—Includes network-wide catastrophic events in the alert. This is the highest severity. • critical—Includes events requiring immediate attention (system log level 1). • debugging—Includes debug events (system log level 7). This is the lowest severity. • disaster—Includes events with significant network impact. • fatal—Includes events where the system is unusable (system log level 0). • major—Includes events classified as major conditions (system log level 2). • minor—Includes events classified as minor conditions (system log level 3) • normal—Specifies the normal state and includes events classified as informational (system log level 6). This is the default. • notification—Includes events informational message events (system log level 5). • warning—Includes events classified as warning conditions (system log level 4).
-----------------	--

Command Default

When you configure the **subscribe-to-alert-group diagnostic** command without specifying any severity, the default is **normal** severity.

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.

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.

Usage Guidelines

To enter call home profile configuration mode, use the **profile (call home)** command in call home configuration mode.

When specifying severity, selecting a lower level severity includes notification of events with any higher severity.



Note

Alert group trigger events and the commands that are executed because of a trigger are platform-dependent. For more information, see the corresponding Call Home configuration documentation for your platform.

Examples

The following example shows how to configure a profile to receive diagnostic alerts for events with severity level 2 or higher:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile example
Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity major
```

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.
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 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 for the Syslog alert group for Call Home.

subscribe-to-alert-group environment

To configure a destination profile to receive messages for the Environment alert group for Call Home, use the **subscribe-to-alert-group environment** command in call home profile configuration mode. To remove the subscription, use the **no** form of this command.

subscribe-to-alert-group environment [severity { **catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}]

no subscribe-to-alert-group environment [severity { **catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}]

Syntax Description

severity	<p>(Optional) Specifies the lowest level of severity events to include in an environment alert, where:</p> <ul style="list-style-type: none"> • catastrophic—Includes network-wide catastrophic events in the alert. This is the highest severity. • critical—Includes events requiring immediate attention (system log level 1). • debugging—Includes debug events (system log level 7). This is the lowest severity. • disaster—Includes events with significant network impact. • fatal—Includes events where the system is unusable (system log level 0). • major—Includes events classified as major conditions (system log level 2). • minor—Includes events classified as minor conditions (system log level 3) • normal—Specifies the normal state and includes events classified as informational (system log level 6). This is the default. • notification—Includes events informational message events (system log level 5). • warning—Includes events classified as warning conditions (system log level 4).
-----------------	--

Command Default

When you configure the **subscribe-to-alert-group environment** command without specifying any severity, the default is **normal** severity.

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.

Release	Modification
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 enter call home profile configuration mode, use the **profile (call home)** command in call home configuration mode.

When specifying severity, selecting a lower level severity includes notification of events with any higher severity.



Note

Alert group trigger events and the commands that are executed because of a trigger are platform-dependent. For more information, see the corresponding Call Home configuration documentation for your platform.

Examples

The following example shows how to configure a profile to receive environment alerts for events with severity level 2 or higher:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile example
Switch(cfg-call-home-profile)# subscribe-to-alert-group environment severity major
```

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.
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 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 for the Syslog alert group for Call Home.

subscribe-to-alert-group inventory

To configure a destination profile to receive messages for the Inventory alert group for Call Home, use the **subscribe-to-alert-group inventory** command in call home profile configuration mode. To remove the subscription, use the **no** form of this command.

```
subscribe-to-alert-group inventory [periodic {daily hh:mm | monthly day hh:mm | weekly day hh:mm}]
```

```
no subscribe-to-alert-group inventory [periodic {daily hh:mm | monthly day hh:mm | weekly day hh:mm}]
```

Syntax Description

periodic	(Optional) Specifies a periodic Call Home message, where: <ul style="list-style-type: none"> • daily hh:mm—Time [in 24-hour format (<i>hh:mm</i>)] for a daily Call Home alert notification to be sent. • monthly day hh:mm—Numeric day of the month (from 1 to 31) and time [in 24-hour format (<i>hh:mm</i>)] for a monthly Call Home alert notification to be sent. • weekly day hh:mm—Day of the week (Monday through Saturday) and time [in 24-hour format (<i>hh:mm</i>)] for a weekly Call Home alert notification to be sent.
-----------------	---

Command Default

This command has no default behavior or values.

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

To enter call home profile configuration mode, use the **profile (call home)** command in call home configuration mode.

When you subscribe to the Inventory alert group without the **periodic** option, a notification occurs whenever a device is cold-booted, or when field-replaceable units (FRUs) are inserted or removed. Otherwise, the notification occurs at the date and time specified.

**Note**

Alert group trigger events and the commands that are executed because of a trigger are platform-dependent. For more information, see the corresponding Call Home configuration documentation for your platform.

Examples

The following example shows how to configure a profile to receive periodic configuration alert notifications every day at 9:12 PM (21:12):

```
Switch(config)# call-home
Switch(cfg-call-home)# profile example
Switch(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 21:12
```

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.
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 syslog	Configures a destination profile to receive messages for the Syslog alert group for Call Home.

subscribe-to-alert-group syslog

To configure a destination profile to receive messages for the Syslog alert group for Call Home, use the **subscribe-to-alert-group syslog** command in call home profile configuration mode. To remove the subscription, use the **no** form of this command.

subscribe-to-alert-group syslog [severity {catastrophic | critical | debugging | disaster | fatal | major | minor | normal | notification | warning} [pattern *match*]]

no subscribe-to-alert-group syslog [severity {catastrophic | critical | debugging | disaster | fatal | major | minor | normal | notification | warning} [pattern *match*]]

Syntax Description

severity	(Optional) Specifies the lowest level of severity events to include in an environment alert, where: <ul style="list-style-type: none"> • catastrophic—Includes network-wide catastrophic events in the alert. This is the highest severity. • critical—Includes events requiring immediate attention (system log level 1). • debugging—Includes debug events (system log level 7). This is the lowest severity. • disaster—Includes events with significant network impact. • fatal—Includes events where the system is unusable (system log level 0). • major—Includes events classified as major conditions (system log level 2). • minor—Includes events classified as minor conditions (system log level 3) • normal—Specifies the normal state and includes events classified as informational (system log level 6). This is the default. • notification—Includes events informational message events (system log level 5). • warning—Includes events classified as warning conditions (system log level 4).
pattern <i>match</i>	(Optional) Specifies a word string in the <i>match</i> argument that should appear in the syslog message to be included in the alert notification. If the pattern contains spaces, you must enclose it in quotes (“ ”).

Command Default

When you configure the **subscribe-to-alert-group syslog** command without specifying any severity, the default is **normal** severity.

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

To enter call home profile configuration mode, use the **profile (call home)** command in call home configuration mode.

You can configure the Syslog alert group to filter messages based on severity and also by specifying a pattern to be matched in the syslog message. If the pattern contains spaces, you must enclose it in quotes (“ ”).

When specifying severity, selecting a lower level severity includes notification of events with any higher severity.

**Note**

Alert group trigger events and the commands that are executed because of a trigger are platform-dependent. For more information, see the corresponding Call Home configuration documentation for your platform.

Examples

The following example shows how to configure a profile to receive syslog alerts for events with severity level 5 or higher, where the syslog message includes the string “UPDOWN”:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile example
Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification
pattern "UPDOWN"
```

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.
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.

timers nsf converge

To adjust the maximum time that a restarting router will wait for the end of table (EOT) notification from a nonstop forwarding (NSF)-capable or NSF-aware peer, use the **timers nsf converge** 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 converge *seconds*

no timers nsf converge

Syntax Description	<i>seconds</i>	Time, in seconds, for which a restarting router will wait for an EOT notification. Valid range is 60 to 180 seconds. The default is 120 seconds.
---------------------------	----------------	--

Command Default	Enhanced Interior Gateway Routing Protocol (EIGRP) NSF awareness is enabled by default. EIGRP NSF awareness uses 120 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)
----------------------	---

Command History	Release	Modification
	12.2(18)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	15.0(1)M	This command was modified. 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 an NSF-capable router. The converge timer is used to wait for the last 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 converge timer on an NSF-capable router. In the example, the converge timer is set to 1 minute:
-----------------	---

```
Router(config-router)# timers nsf converge 60
```

The following EIGRP named configuration example adjusts the converge timer on an NSF-capable router. In the example, the converge timer is set to 1 minute:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# timers nsf converge 60
```

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 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.
timers nsf signal	Adjusts the maximum time for the initial restart period.

timers nsf route-hold



Note

Effective with Cisco IOS Release 15.0(1)M and 12.2(33)SRE, the **timers nsf route-hold** command was replaced by the **timers graceful-restart purge-time** command. See the **timers graceful-restart purge-time** command for more information.

To set the route-hold timer to determine how long a nonstop forwarding (NSF)-aware router that is running Enhanced Interior Gateway Routing Protocol (EIGRP) will hold routes for an inactive peer, use the **timers nsf route-hold** command in router configuration mode. To return the route-hold timer to the default value, use the **no** form of this command.

timers nsf route-hold *seconds*

no timers nsf route-hold

Syntax Description

<i>seconds</i>	Time, in seconds, for which EIGRP will hold routes for an inactive peer. Valid range is 20 to 300 seconds. The default is 240 seconds.
----------------	--

Command Default

EIGRP NSF awareness is enabled by default. The default value for the route-hold timer is 240 seconds.

Command Modes

Router configuration (config-router)

Command History

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 replaced by the timers graceful-restart purge-time command.
12.2(33)SRE	This command was replaced by the timers graceful-restart purge-time command.

Usage Guidelines

The route-hold timer sets the maximum period of time that the NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

Examples

The following configuration example sets the route-hold timer value for an NSF-aware router. In the example, the route-hold timer is set to 2 minutes:

```
Router(config-router)# timers nsf route-hold 120
```

Related Commands

Command	Description
debug eigrp nsf	Displays EIGRP NSF-specific events in the console of a router.
debug ip eigrp notifications	Displays EIGRP events and notifications in the console of the router.
show ip eigrp neighbors	Displays the neighbors discovered by IP EIGRP.
show ip protocols	Displays the parameters and current state of the active routing protocol process.

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

<i>seconds</i>	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)

Command History

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

<i>name</i>	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)

Command History

Release	Modification
12.2(33)SX11	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)

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.

