show call-home through vrrp sso

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** | **events**}]

Syntax Description

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

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.
Cisco IOS XE Release 16.6.1	This command was integrated into Cisco IOS XE Release 16..6.1

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
```

The following example displays information for all call-home registered events:

```
Router# show call-home events

 Active event list:
 Profile                        Alert Group     Internal Index  Severity       Subscription
  Last Triggered Time

-------------------------------------------------------------------------------------------------

 tst                            configuration  1     /1         normal         normal
   2017-08-08 08:45:09 GMT+00:00
 tst                            test           2     /2         normal         normal

 tst                            crash          3     /3         debug          normal

 tst                            crash          4     /4         debug          normal

 tst                            inventory      5     /5         normal         normal

 tst                            inventory      6     /6         normal         normal

 tst                            syslog         7     /7         debug          pattern
   2017-08-08 08:45:09 GMT+00:00
 tst                            configuration  8     /8         normal         periodic

 tst                            syslog         9     /9         catastrophic   pattern

ultra01#
```

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 call-home diagnostic-signature

To display the attributes and statistics of a call-home diagnostic signature file that is available on a device, use the **show call-home diagnostic-signature** command in privileged EXEC mode.

show call-home diagnostic-signature [{*ds-id* [{**actions** | **events** | **prerequisite** | **prompt** | **variables**}] | **failure** | **statistics** [**download**]}]

Syntax Description

ds-id	(Optional) Name, functionality, event, and action that is associated with the specified diagnostic signature ID.
actions	(Optional) Displays the diagnostic signature actions associated with the specified diagnostic signature ID.
events	(Optional) Displays the diagnostic signature events associated with the specified diagnostic signature ID.
prerequisite	(Optional) Displays the diagnostic signature prerequisites associated with the specified diagnostic signature ID.
prompt	(Optional) Displays the diagnostic signature prompts associated with the specified diagnostic signature ID.
variables	(Optional) Displays the diagnostic signature environment variables associated with the specified diagnostic signature ID.
failure	(Optional) Displays all malfunctioned diagnostic signature files at various stages such as downloading, parsing, file saving, acting, registration, sign verification, and unknown. **Note** The failure history is not retained after the device reloads.
statistics	(Optional) Displays statistics for all diagnostic signature IDs on a device. The statistics include diagnostic signature average run time, maximum run time, and the number of times the diagnostic signature was triggered, uninstalled, or maximum triggered times limit; associated with all diagnostic signature IDs on the device.
download	(Optional) Displays the diagnostic signature download statistics for periodic and on-demand type of downloads.

Command Default

If you do not specify any optional keywords and arguments, only the current diagnostic signature settings such as diagnostic signature status (enabled or disabled), profile, and environment variable, along with details associated with the downloaded diagnostic signature files, such as the diagnostic signature name, revision number, status, and last updated date and time are displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show call-home diagnostic-signature** *ds-id* command to display all attributes, such as, ID, name, functionality, event, action, prerequisites, prompts, and variables that are associated with a diagnostic signature file. If you want to view a particular aspect of the diagnostic signature file, use any of the optional keywords (**actions**, **events**, **prerequisite**, **prompt**, or **variables**) with the *ds-id* argument.

Use the **show call-home diagnostic-signature failure** command to display any malfunctions that occur with a diagnostic signature file or a set of diagnostic signature files during any of the following stages:

- Downloading—The diagnostic signature fails while being downloaded onto a device.
- Parsing—The diagnostic signature fails during parsing.
- File saving—The diagnostic signature fails during file saving.
- Acting—The diagnostic signature fails while performing an action on the device.
- Unknown—The diagnostic signature fails due to an unknown factor.
- Registration—The diagnostic signature fails during registration on a device.
- Sign verification—The diagnostic signature fails during digital signature verification.

Example

The following is sample output from the **show call-home diagnostic-signature** command. The command output displays the active diagnostic signature profile prof-1, environment variable name ds_env1, and environment variable value value1.

```
Device# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: prof-1 (status: ACTIVE)
Environment variable: ds_env1: value1
Downloaded DSes:
DS ID    DS Name                          Revision Status     Last Update (GMT+00:00)
-------- -------------------------------- -------- ---------- -------------------
6015     CronInterval                     1.0      registered 2013-01-16 04:49:52
6030     ActCH                            1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                      1.0      registered 2013-01-16 06:10:37
6033     PureTCL                          1.0      registered 2013-01-16 06:11:48
```

Following is sample output from the **show call-home diagnostic-signature** command with the *ds-id* argument value as 6015:

```
Device# show call-home diagnostic-signature 6015

ID              : 6015
Name            : CronInterval
Functionality   :
Send call-home message every 3 minutes with cron timer.
Event           :
Event Tag       : e1
Type            : periodic
Timer Type      : cron
Timer Detail    : */3 * * * *
Includes action steps that may impact device state: No
Action          :
Type            : CALLHOME
```

```
Element List    :
DATA            : show clock
DATA            : show version
```

The following sample output from the **show call-home diagnostic-signature statistics** command displays various diagnostic signature IDs:

```
Device# show call-home diagnostic-signature statistics

DS ID     DS Name                     Triggered/Max/Deinstall     Average               Max

                                                                 Run Time(sec)       Run
Time(sec)
--------  --------------------------     -------------        -------------     -----------
6015      CronInterval                     4/0/N                 9.872              9.981
6030      ActCH                             932/0/N               13.333
1357.860
6032      MultiEvents                      10/0/N                6.362              6.692
6033      PureTCL                          15/0/N                6.363              7.620
```

The following is sample output from the **show call-home diagnostic-signature statistics download** command:

```
Device# show call-home diagnostic-signature statistics download

Download-type    In-queue      Fail    Success   Last request sent
-------------   ----------    -----   ---------  ----------------------------
Periodic            0          0        0
Ondemand            0          1        1        2013-01-16 04:49:52 GMT+00:00
```

The following is sample output from the **show call-home diagnostic-signature failure** command:

```
Device# show call-home diagnostic-signature failure

Stage: D - Download, P - Parsing, F - File saving, A - Acting, U - Unknown
       R - Registration, S - Sign verification
                                        Last Failed Time
DS ID    DS Name          Stage            (GMT+08:00)            Error String
-------- ---------------- -----     -------------------         ---------------------------
100      OirEvents        P            2012-03-08 12:02:59          Call Home error

200      OirEvents        P            2012-03-08 12:02:59          Call Home error
```

The following table describes the significant fields in the order in which they appear in the displays.

Table 1: show call-home diagnostic-signature Field Descriptions

Field	Description
Profile	The call-home destination profile associated with the diagnostic signature on a device.
Environment variable	The environment variable that is set up for a diagnostic signature on a device.
DS ID	The diagnostic signature identification number as saved on the HTTP/HTTPS servers.
DS Name	The diagnostic signature name, assigned to the diagnostic signature file.

Field	Description
Revision	The diagnostic signature file version number that indicates if the signature file is new or updated.
Status	Possible statuses for a downloaded call-home diagnostic signature file are: • registered—The diagnostic signature monitors and registers the predefined events and waits for such events to occur. • running—The diagnostic signature executes the specified actions for events that are registered. • terminated—The diagnostic signature is terminated and unregistered when a diagnostic signature has performed the specified action for the maximum number of times. • pending—The diagnostic signature is in a pending state when some required environment variable has no value configured. In the case of an interactive diagnostic signature, it must be manually installed using the **call-home diagnostic-signature install** command.
Last Update	The date and time when the diagnostic signature file was last updated on the device through periodic or on-demand download.
Functionality • event trigger • action	The functionality of a particular diagnostic signature file. • The event trigger indicates the event when the diagnostic signature performs a specific action. • The action indicates the specific action that the diagnostic signature performs when an event occurs.
Event • Event tag • Type • Timer Type • Timer Detail	The event details defined within the diagnostic signature file. • Event tag indicates the event name. • Type indicates whether the event is checked for periodically or if the check is on an on-demand basis. • Timer Type and Timer Detail indicate the clock system and the time period assigned to check for the event.

Field	Description
Action • Type • Element List • DATA	The action defined within the diagnostic signature file. • Type indicates the kind of action that is performed in response to a certain event. • Element List and DATA indicate the various aspects of the device that are affected when the action is performed.
Triggered/Max/Deinstall	• Triggered indicates the number of times a specific diagnostic signature was performed. • Max indicates the number of times specific diagnostic signature files are limit from being performed. • Deinstall indicates whether or not a particular diagnostic signature was subjected to uninstallation.
Average Run Time (sec)	The average time, in seconds, taken for a particular diagnostic signature file to execute its actions in response to the predefined events across various sessions on a device.
Max Run Time (sec)	The maximum time, in seconds, taken for a particular diagnostic signature file to perform its action in response to the predefined event for a particular session on a device.
Download-type	Type of downloading method for diagnostic signature files; either periodic or on-demand. • Periodic indicates that the diagnostic signature file downloading type is periodic, that is, the device is configured to automatically request for the download of new or updated diagnostic signature files at regular intervals. • Ondemand indicates that the diagnostic signature file downloading type is on-demand, that is, the device must be manually configured to request for the download of new or updated diagnostic signature files.
In-queue	Indicates the number of diagnostic signature files that are in the queue waiting to be downloaded on to the device. 0 indicates there are no files waiting in the queue.

Field	Description
Fail	Indicates the number of diagnostic signature files that failed while downloading. 0 indicates there is no failure during the download.
Success	Indicates the number of diagnostic signature files that are successfully downloaded on to the device. 0 indicates no files have been downloaded.
Last request sent	The date and time when the last request for download was initiated from the device.
Stage • D—Download • P—Parsing • F—File saving • A—Acting • U—Unknown • R—Registration • S—Sign Verification	Indicates the stage when the diagnostic signature failed.
Last Failed Time	Indicates the date and time when the diagnostic signature failed.
Error String	Indicates the errors associated with the diagnostic signature failure.

Related Commands

Command	Description
call-home diagnostic-signature	Downloads, installs, and uninstalls diagnostic signature files on a device.
diagnostic-signature	Enables the diagnostic signature feature on a device.

show cef nsf

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

show cef nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

The following example shows the current NSF state:

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

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

Table 2: 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(20T, 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
```

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

Table 3: 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
```

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

Table 4: 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 vpn4 sso summary** command in privileged EXEC mode.

show ip bgp vpnv4 all sso summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE 3.7S	This command was implemented on the Cisco ASR 903 router.

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
```

The table below describes the fields shown in the display.

Table 5: 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.
15.2(2)S	This command was modified. The output was enhanced to show checkpoint information for MPLS traffic engineering autotunnel and automesh stateful switchover (SSO) tunnels.
Cisco IOS XE Release 3.6S	This command was modified. The output was enhanced to show checkpoint information for MPLS traffic engineering autotunnel and automesh stateful switchover (SSO) tunnels.

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
```

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

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

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

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

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

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

State: Standby

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

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

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

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

  Init:
    Succeeded:            1
    Failed:               0

  Session Registration:
    Succeeded:            0
    Failed:               0

  Session Unregistration:
    Succeeded:            0
    Failed:               0

Errors:
  None
```

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

Table 7: show ip rsvp high-availability counters—Standby RP Field Descriptions

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

Related Commands

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

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

show ip rsvp interface detail

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

show ip rsvp interface detail [*type number*]

Syntax Description

type number	(Optional) The type and number of the interface for which you want to display the hello configuration.

Command Default

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.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

To display the hello configuration for a specific interface, use the **show ip rsvp interface detail** command with the *type* and *number* arguments.

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
```

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

Table 8: show ip rsvp interface detail Field Descriptions

Field	Description
RSVP	Status of the Resource Reservation Protocol (RSVP) (Enabled or Disabled).
Interface State	Status of the interface (Up or Down).
Curr allocated	Amount of bandwidth (in bits per second [b/s]) currently allocated.
Max. allowed (total)	Total maximum amount of bandwidth (in b/s) allowed.
Max. allowed (per flow)	Maximum amount of bandwidth (in b/s) allowed per flow.
Max. allowed for LSP tunnels using sub-pools	Maximum amount of bandwidth permitted for the 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 in the RSVP messages.

show isis nsf

To display current state information regarding Intermediate System-to-Intermediate System (IS-IS) Cisco nonstop forwarding (NSF), use the **s how 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
```

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

Table 9: 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.

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 eSFU 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 EHSA 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
```

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

Table 10: show issu clients Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for that client.

Field	Description
Client_Name	A character string describing the client. "Base Clients" are a subset, which includes: • Inter-Process Communications (IPC) • Redundancy Framework (RF) • Checkpoint Facility (CF) • Cisco Express Forwarding • Network RF (for IDB stateful switchover) • EHSA 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** | **xml**}

Syntax Description

negotiated	Displays ISSU negotiated matrix information.
stored	Displays ISSU stored matrix information.
xml	Displays ISSU XML 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	This command was integrated into Cisco IOS Release 12.2(33)SRB1. Support for ISSU was introduced on the Cisco 7600 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Perform an ISSU when the Cisco software on both the active and the standby RP is capable of ISSU and the old and new images are compatible. The compatibility matrix information stores the compatibility among releases in the following manner:

- Compatible—The base-level system infrastructure and all optional High Availability (HA) aware subsystems are compatible. An in-service upgrade or downgrade between these versions will succeed with minimal service impact. The matrix entry designates the images to be compatible ©).
- Base-level compatible—One or more of the optional HA-aware subsystems is not compatible. An in-service upgrade or downgrade between these versions will succeed; however, some subsystems will not be able to maintain state during the transition. The matrix entry designates the images to be base-level compatible (B). You can perform an ISSU upgrade without any functionality loss even if the matrix entry is B. However, you might experience some functionality loss with a downgrade, if the new image has additional functionality.
- Incompatible—A core set of system infrastructure exists that interoperates in a stateful manner for SSO to function correctly. If any of these required features or protocols is not interoperable, the two versions of the Cisco software images are declared to be incompatible. An in-service upgrade or downgrade between these versions is not possible. The matrix entry designates the images to be incompatible (I). When the Cisco IOS versions at the active and standby supervisor engines are incompatible, the system operates in route processor redundancy (RPR) mode.

Note when you try to perform an ISSU with a peer that does not support ISSU, the system automatically uses RPR mode.

The compatibility matrix represents the compatibility relationship a Cisco software image has with all other Cisco software versions within the designated support window (for example, all the software versions the image is aware of) and is populated and released with every image. The matrix stores compatibility information between its own release and prior releases. It is always the current release that contains latest information about compatibility with existing releases in the field. The compatibility matrix is available within the Cisco software image and on Cisco.com so that users can determine in advance whether an upgrade can be done using the ISSU process.

Use the **show issu comp-matrix negotiated** command to display information on the negotiation of the compatibility matrix data between two software versions on a device.

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

Examples

The following is sample output from the **show issu comp-matrix negotiated** command:

```
Device# show issu comp-matrix negotiated

CardType: C10008(107), Uid: 1,  Image Ver: 12.2(31)SB2
Image Name: C10K2-P11-M

Cid     Eid     Sid     pSid    pUid      Compatibility
=========================================================
2       1       4       4       2         COMPATIBLE
3       1       65549   6       2         COMPATIBLE
4       1       17      14      2         COMPATIBLE
5       1       49      44      2         COMPATIBLE
7       1       5       5       2         COMPATIBLE
8       1       65545   11      2         COMPATIBLE
9       1       2       2       2         COMPATIBLE
9       1       47      0       1         COMPATIBLE
9       1       87      0       1         COMPATIBLE
9       1       65548   0       1         COMPATIBLE
10      1       3       3       2         COMPATIBLE
10      1       48      0       1         COMPATIBLE
10      1       88      0       1         COMPATIBLE
10      1       65547   0       1         COMPATIBLE

Message group summary:
Cid     Eid     GrpId     Sid     pSid    pUid    Nego Result
============================================================
2       1       1         4       4       2       Y
3       1       1         65549   6       2       Y
4       1       1         17      14      2       Y
5       1       1         49      44      2       Y
7       1       1         5       5       2       Y
8       1       1         65545   11      2       Y
9       1       1         2       2       2       Y
9       1       1         47      0       1       Y
9       1       1         87      0       1       Y
9       1       1         65548   0       1       Y
10      1       1         3       3       2       Y
10      1       1         48      0       1       Y
10      1       1         88      0       1       Y
```

```
10      1       1         65547   0       1       Y

List of Clients:
Cid       Client Name              Base/Non-Base
==============================================
2         ISSU Proto client        Base
3         ISSU RF                  Base
4         ISSU CF client           Base
5         ISSU Network RF client   Base
7         ISSU CONFIG SYNC         Base
8         ISSU ifIndex sync        Base
9         ISSU IPC client          Base
10        ISSU IPC Server client   Base
```

The following is sample output from the **show issu comp-matrix stored** command:

```
Device# show issu comp-matrix stored

Number of Matrices in Table = 1

        (1) Matrix for C10K2-P11-M(107) - C10K2-P11-M(107)
        ==========================================
        Start Flag (0xDEADBABE)

                My Image ver:  12.2(31)SB2
                Peer Version    Compatability
                ------------    -------------
                12.2(27)SBB1            Base(2)
                12.2(27)SBB4            Base(2)
                12.2(27)SBB5            Base(2)
                12.2(27)SBB6            Base(2)
                12.2(27)SBB7            Base(2)
                12.2(28)SB5             Base(2)
                12.2(31)SB2             Comp(3)
```

The following is sample output from the **show issu comp-matrix xml** command:

```
Device# show issu comp-matrix xml

<endpoint_info uid="1">
<CardDescription>
<CardType>C10008</CardType>  <cardtype_num>107</cardtype_num>  <uid>1</uid>
<image type="imagename-release-split">
<image-name>C10K2-P11-M</image-name>
<release-number>12.2(31)SB2</release-number>
</image>
</CardDescription>

<ClientTable>
<client_entry cid ="2">
<client_id>2</client_id> <entity_id>1</entity_id> <session_id>4</session_id>
<peer_session_id>4</peer_session_id> <peer_uid>2</peer_uid>
<compatibility><level>COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="3">
<client_id>3</client_id> <entity_id>1</entity_id> <session_id>65549</session_id>
<peer_session_id>6</peer_session_id> <peer_uid>2</peer_uid>
<compatibility><level>COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="4">
<client_id>4</client_id> <entity_id>1</entity_id> <session_id>17</session_id>
<peer_session_id>14</peer_session_id> <peer_uid>2</peer_uid>
<compatibility><level>COMPATIBLE</level></compatibility>
```

```
COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="5">
<client_id>5</client_id> <entity_id>1</entity_id> <session_id>49</session_id>
<peer_session_id>44</peer_session_id>
<peer_uid>2</peer_uid> <compatibility><level>COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="7">
<client_id>7</client_id> <entity_id>1</entity_id> <session_id>5</session_id>
<peer_session_id>5</peer_session_id>
<peer_uid>2</peer_uid> <compatibility><level>COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="8">
<client_id>8</client_id> <entity_id>1</entity_id> <session_id>65545</session_id>
<peer_session_id>11</peer_session_id>
<peer_uid>2</peer_uid> <compatibility><level>COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="9">
<client_id>9</client_id> <entity_id>1</entity_id> <session_id>2</session_id>
<peer_session_id>2</peer_session_id>
<peer_uid>2</peer_uid> <compatibility><level>COMPATIBLE</level></compatibility>
</client_entry>
<client_entry cid ="10">
<client_id>10</client_id> <entity_id>1</entity_id> <session_id>3</session_id>
<peer_session_id>3</peer_session_id>
<peer_uid>2</peer_uid> <compatibility><level>COMPATIBLE</level></compatibility>
```

The following table describes the significant fields in the order in which they appear in the displays.

Table 11: show issu comp-matrix Field Description

Field	Description
CardType	The type of line card installed in the slot.
Uid	The unique identification number for the current endpoint.
Image Ver	The image verison installed on the device.
Image Name	The name of the image installed on the device.
Cid	The identification number used by ISSU for the client.
Eid	The identification number used by ISSU for each entity within this client.
Sid	The identification number of the session being reported on.
pSid	The peer session ID at the other endpoint.
pUid	The peer unique ID on the other endpoint where the session terminates.
Compatibility	The compatibility status means that the ISSU session is compatible.
GrpId	The group ID number of the message group used for the session.
Client Name	The client name used for the image to interoperate.
Base/Non-Base	The client required for the image to interoperate.

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 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
```

The tabl below describes the significant field shown in the display.

Table 12: 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.
MsgGroup Count	The number of message groups within the identified entity. A message group is a list of message types.

Field	Description
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
```

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

Table 13: 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.
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.

Field	Description
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	Displays results of a negotiation about versions of the messages exchanged during the specified session, between the active and standby endpoints.
capability	Displays results of a negotiation about the client application's capabilities for the specified session.
session-id	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
```

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

Table 14: 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.
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
```

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

Table 15: 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

slot-num	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#
```

The table below describes the fields in the display.

Table 16: 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: • 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.
disk	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
```

The table below describes significant fields shown in the display.

Table 17: 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.

Command Default

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
```

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

Table 18: 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.
No. of MDR feasible cards:1	Total number of nonlegacy line cards that are one of the following types: • VIP 4-50 controller • VIP 4-80 controller • VIP 6-80 controller • GEIP+ controller.

Field	Description
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.

Command	Description
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	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
```

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

Table 19: 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

client-id	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
```

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

Table 20: 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.

Field	Description
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

slot	(Optional) PRE slot number.
port	(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
1gigethernet-hh-1        NO ACTION         0x00000200
```

The table below 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 21: 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.

Field	Description
RP State = Standby	State of this RP.
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#
```

The table below describes the fields in the display.

Table 22: 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**}

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.
minutes	Time argument in minutes. The time argument is specified in minutes format (mmm).
hours **:** *minutes*	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).
day month	(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.
seconds	(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
```

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

Table 23: 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 display 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.

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

Table 24: 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.

Command Default

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
```

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

Table 25: show mpls ip iprm counters Command Field Descriptions

Field	Description
CEF Tree Changes Processed/Ignored	Processed--The number of Cisco Express Forwarding tree change announcements that IPRM processed. Ignored--The number of Cisco Express Forwarding tree change announcements that IPRM ignored. Typically, IPRM processes tree change announcements only for prefixes in a routing table.
CEF Deletes Processed/Ignored	Processed--The number of Cisco Express Forwarding delete entry announcements that IPRM processed. Ignored--The number of Cisco Express Forwarding delete entry announcements that IPRM ignored. Typically, IPRM processes delete entry announcements only for prefixes in a routing table.
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	Successes--The number of times IPRM successfully updated the MPLS forwarding information. Failures--The number of times IPRM attempted to update the MPLS forwarding information and failed.
Rewrite Gets/Deletes	Gets--The number of times IPRM retrieved forwarding information from the MPLS forwarding infrastructure. Deletes--The number of times IPRM removed prefix forwarding information from the MPLS forwarding infrastructure.
Label Announcements: Info/Local/Path	Info--The number of times an IP label distribution module informed IPRM that label information for a prefix changed. Local--The number of times an IP label distribution module specified local labels for a prefix. Path--The number of times an IP LDM specified outgoing labels for a prefix route.
Walks: Recursion Tree/CEF Full/CEF interface	Recursion Tree--The number of times IPRM requested Cisco Express Forwarding to walk the recursion (path) tree for a prefix. CEF Full--The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix. 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.

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.
table-id	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.
vrf-name	(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.

Command Default

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 (glbl;ipv4); ldms: 2
    lcatm, ldp
  table (glbl;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 vpnv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all
  table (glbl;ipv4); ldms: 2
    lcatm, ldp
  table (glbl;ipv6); ldms: 1
    bgp ipv6
  table (all-tbls;ipv4); ldms: 1
    bgp vpnv4
```

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

```
Router# show mpls ip iprm ldm ipv6
  table (glbl;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 (glbl;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 vpnv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all
  table (glbl;ipv4); ldms: 1
    ldp
  table (all-tbls;ipv4); ldms: 1
    bgp vpnv4
```

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** | **inter-device** | **states** | **switchover** | **switchover history**}]

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.
inter-device	(Optional) Displays redundancy interdevice operational state and statistics.
states	(Optional) Displays redundancy-related states: disabled, initialization, standby, active (various substates for the latter two), client ID and name, length of time since the 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.
switchover history	(Optional) Displays redundancy switchover history.

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 modified. This command was made available 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.

Release	Modification
12.2(14)SX	The user EXEC mode form of this command was implemented on the Supervisor Engine 720.
12.2(18)S	This command was implemented on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(20)S	The **states**, **counters**, **clients**, **history**, and **switchover history** keywords were added.
12.2(17d)SXB	Support for the user EXEC mode form of this command was extended to the Supervisor Engine 2.
12.3(8)T	The **inter-device** keyword was added to the privileged EXEC form of the command.
12.3(11)T	The user EXEC form of this command was integrated into Cisco IOS Release 12.3(11)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	The **clients** keyword was enhanced to provide information about the status of each client.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.
12.2(31)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	More information regarding the **states** keyword was added.

Usage Guidelines

Cisco AS5800

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

Cisco AS5850

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

Examples

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

```
Router# show redundancy clients
 clientID = 0       clientSeq = 0        RF_INTERNAL_MSG
 clientID = 25      clientSeq = 130      CHKPT RF
 clientID = 5026    clientSeq = 130      CHKPT RF
 clientID = 5029    clientSeq = 135      Redundancy Mode RF
```

```
clientID = 5006    clientSeq = 170      RFS client
clientID = 6       clientSeq = 180      Const OIR Client
clientID = 7       clientSeq = 190      PF Client
clientID = 5008    clientSeq = 190      PF Client
clientID = 28      clientSeq = 330      Const Startup Config
clientID = 29      clientSeq = 340      Const IDPROM Client
clientID = 65000   clientSeq = 65000    RF_LAST_CLIENT
```

The output displays the following information:

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

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

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

The following example shows information about the RF history:

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

The following example shows information about the RF state:

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 1
```

```
Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured)  = Route Processor Redundancy
     Split Mode = Disabled
   Manual Swact = Disabled  Reason: Simplex mode
 Communications = Down      Reason: Simplex mode
   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0
```

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

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

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

Example: Setting the terminal length for the Cisco ASR 1006

The following example shows how to set the terminal length value to pause the multiple-screen output:

```
Router# terminal length 5
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 48
```

Example: Cisco AS5850

The following is sample output from the **show redundancy handover** and **show redundancy states** commands on the 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
```

Example: Cisco AS5800

The following is sample output from the **show redundancy** command on the 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.
```

Example: Cisco AS5800 with History

The following is sample output from the **show redundancy history** command on the 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
```

Example: Cisco AS5800 Router Shelves as Failover Pair

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 the**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
```

Example: Privileged EXEC Mode

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

```
RouterB# show redundancy
MWR1900 is the Active Router
Previous States with most recent at bottom
 INITL_INITL     Dec 31 19:00:00.000
 LISTN_INITL     Feb 28 19:00:15.568
```

```
LISTN_LISTN     Feb 28 19:00:15.568
SPEAK_LISTN     Feb 28 19:00:18.568
SPEAK_SPEAK     Feb 28 19:00:18.568
STDBY_SPEAK     Mar 19 08:54:26.191
ACTIV_SPEAK     Mar 19 08:54:26.191
ACTIV_STDBY     Mar 19 08:54:26.191
ACTIV_ACTIV     Mar 19 08:54:26.191
INITL_ACTIV     Mar 19 08:56:22.700
INITL_INITL     Mar 19 08:56:22.700
INITL_LISTN     Mar 19 08:56:28.544
LISTN_LISTN     Mar 19 08:56:28.652
LISTN_SPEAK     Mar 19 08:56:31.544
SPEAK_SPEAK     Mar 19 08:56:31.652
SPEAK_STDBY     Mar 19 08:56:34.544
SPEAK_ACTIV     Mar 19 08:56:34.544
STDBY_ACTIV     Mar 19 08:56:34.652
ACTIV_ACTIV     Mar 19 08:56:34.652
INITL_ACTIV     Mar 19 10:20:41.455
INITL_INITL     Mar 19 10:20:41.455
INITL_LISTN     Mar 19 10:20:49.243
LISTN_LISTN     Mar 19 10:20:49.299
LISTN_SPEAK     Mar 19 10:20:52.244
SPEAK_SPEAK     Mar 19 10:20:52.300
SPEAK_STDBY     Mar 19 10:20:55.244
STDBY_STDBY     Mar 19 10:20:55.300
ACTIV_STDBY     Mar 19 10:21:01.692
ACTIV_ACTIV     Mar 19 10:21:01.692
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) router shelves (Cisco AS5800) or RSCs (Cisco AS5850).
hw-module	Enables the router shelf to stop a DSC or to restart a stopped DSC.
mode	Sets the redundancy mode.
mode y-cable	Invokes y-cable mode.
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
show chassis	Displays, for a router with two RSCs, information about the 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
```

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

Table 26: 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)	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. • 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.

show tcp ha statistics

To display statistical information for the TCP High Availability (HA) connection, use the **show tcp ha statistics** command in privileged EXEC mode.

show tcp ha statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.2(1)S	This command was modified. Additional TCP counters and HA statistics for troubleshooting Nonstop Routing (NSR) were added to the output.

Examples

Cisco IOS Release 15.2(1)S and later releases

The following sample output displays the statistics for the TCP HA connection at the active device, including additional counters for failures:

```
Router# show tcp ha statistics
TCP HA statistics (active)
        TCP HA statistics (active)
        69 total messages sent successfully
        0 total messages received successfully
        0 total messages failed (IPC layer)
        45 packets (incoming) punted
        1 packets (with ISN) punted
        23 send_msg packets sent
        45 (incoming) packets ACKed from standby
        23 (outgoing) send_msg ACKed from standby
        0 app messages fragmented
        0 recv buff sent
        0 app messages > mss
        0 total feedback decoded
        0 total remove connection encoded
        0 total new conn ipv4 encoded
        0 total send var encoded
        0 total recv var encoded
        0 total rtt encoded
        0 total options encoded
        0 total send queue encoded
        0 total sync done encoded
        0 messages sent beyond flowcontrol
        0 total failure messages encoded
        0 total failure messages decoded
        0 failure communication with standby
        0 failure assymetric startup
        0 failure notify handler not set
        0 failure notify app
```

The following sample output displays the statistics for the TCP HA connection at the standby device:

```
Router# show tcp ha statistics
TCP HA statistics (standby)
    69 total messages received
    45 packets received
    1 packets (with ISN) received
    23 send_msg packets received
    0 fragments received
    0 recv buff received
    0 remove conn decoded
    0 new_conn_ipv4_decoded decoded
    0 rtt decoded
    0 send_var decoded
    0 recv_var decoded
    0 stats decoded
    0 options decoded
    0 send_queue decoded
    0 sync_done decoded
    0 sync_done_fdbk decoded
    0 failure message encoded
    0 failure message decoded
    0 failure malloc
    0 failure getbuffer
    0 failure invalid tcb
    0 failure window closed
    0 failure no app data
    0 failure add tcb
    0 failure no options
    0 failure no listener
    0 failure cant inform app
    0 failure communication with active
```

Cisco IOS Release 15.1(3)S and earlier releases

The following sample output displays the statistics for the TCP HA connection at the active device:

```
Router# show tcp ha statistics
TCP HA statistics (active)
        71 total messages sent successfully
        1 total messages received successfully
        0 total messages failed
        41 packets (incoming) punted
        0 packets (with ISN) punted
        23 send_msg packets sent
        41 (incoming) packets ACKed from standby
        23 (outgoing) send_msg ACKed from standby
        0 app messages fragmented
        1 recv buff sent
        0 app messages > mss
```

The following sample output displays the statistics for the TCP HA connection at the standby device:

```
Router-1# show tcp ha statistics
TCP HA statistics (standby)
        87 total messages received
        51 packets received
        0 packets (with ISN) received
        29 send_msg packets received
        0 fragments received
        1 recv buff received
```

Related Commands

Command	Description
show tcp ha connections	Displays connection-ID-to-TCP mapping data.

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

alphanumeric	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 Site1ManhattenNY
```

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 Manhatten 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.[2]
	• **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: [3]
	  • **boot-up-fail**--(Optional) Enables the SNMP ceDiagBootUpFailedNotif traps.
	  • **hm-test-recover**--(Optional) Enables the SNMP ceDiagHMTestRecoverNotif traps.
	  • **hm-thresh-reached**--(Optional) Enables the SNMP ceDiagHMThresholdReachedNotif traps.
	  • **scheduled-fail**--(Optional) Enables the SNMP ceDiagScheduledJobFailedNotif traps.

	• **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. [4]
	• **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. [5]
	• **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.
[2] Supported on the Catalyst 6500 series switches.
[3] Supported on the Catalyst 6500 series switches.
[4] Supported on the Catalyst 6500 series switches.
[5] 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.

Release	Modification
12.4(4)T	Support for the **alarms** *severity* notification type and 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.
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: **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.

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.

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 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.

Command	Description
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-server 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.

source-interface

To specify the name of the source interface that the Call-Home service uses to send out e-mail messages, use the **source-interface** command in call home configuration mode.

source-interface *interface-name*
no source-interface

Syntax Description

interface-name	Source-interface name. Maximum length is 64.

Command Default

Call-Home service sends out the e-mail messages using the packet outbound interface as its source interface.

Command Modes

Call home configuration (cfg-call-home)

Command History

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

Usage Guidelines

You can specify either the source-interface name or the source-ip-address when sending Call-Home e-mail messages but not both. The Call-Home service sends out a warning when either the source-interface name or the source-ip-address has already been configured and you attempt to configure one of these options again. If neither of these two are specified, the Call-Home service uses the outbound interface as its source interface and uses that interface's IP address as the source IP address to send out the e-mail messages.

If the specified source interface's status is up and has at least one IP address configured when the Call-Home message is sent out, the e-mail message shows the source interface's IP address. To verify the IP address, use the **debug call-home mail** command or select the e-mail Internet headers option. When the specified source interface is down or has no IP address configured, the Call-Home message is not sent out.

Note For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.

Examples

The following example specifies loopback1 as the name of the source interface that the Call-Home service uses to send out e-mail messages:

```
Router(cfg-call-home)# source-interface loopback1
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.
ip http client source-interface	Specifies the source interface name for HTTP messages.

Command	Description
source-ip-address	Specifies the source IP address with which the Call-Home e-mail messages are sent out.

source-ip-address

To specify the source IP address with which the Call-Home e-mail messages are sent out, use the **source-ip-address** command in call home configuration mode.

no source-ip-address {**ipv4 address** | **/ipv6 address**}
no source-ip-address

Syntax Description

ipv4 address | **/ipv6 address**	Source IP (ipv4 or ipv6) address. Maximum length is 64.

Command Default

Call-Home service sends out the e-mail messages using the IP address of the outbound interface as its source IP address.

Command Modes

Call home configuration (cfg-call-home)

Command History

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

Usage Guidelines

You can specify either the source-interface name or the source-ip-address when sending Call-Home e-mail messages but not both. The Call-Home service sends out a warning when either the source-interface name or the source-ip-address has already been configured and you attempt to configure one of these options again. If neither of these two are specified, the Call-Home service uses the IP address configured on the message outbound interface as source IP address to send the e-mail message out.

If the specified source-ip-address is also configured as an IP address of any workable device interface when the Call-Home message is sent out, the e-mail message uses it as its source IP address. To verify the IP address, use the **debug call-home mail**command or select the e-mail Internet headers option. When the specified source-ip-address is not any of the IP addresses configured on workable interfaces, the Call-Home message is not sent out.

Note For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.

Examples

The following example specifies 209.165.200.226 as the source IP address that the Call-Home service uses to send out e-mail messages:

```
Router(cfg-call-home)# source-ip-address 209.165.200.226
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

Command	Description
ip http client source-interface	Specifies the source interface name for HTTP messages.
source-interface	Specifies the name of the source interface that the Call-Home service uses to send out e-mail messages.

show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.

show ip bgp [{*ip-address* [{*mask* [{**longer-prefixes** [{**injected**}] | **shorter-prefixes** [{*length*}] | **best-path-reason** | **bestpath** | **multipaths** | **subnets**}] | **best-path-reason** | **bestpath** | **multipaths**}] | **all** | **oer-paths** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name* | **version** {*version-number* | **recent** *offset-value*}}]

Syntax Description

ip-address	(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.
mask	(Optional) Mask to filter or match hosts that are part of the specified network.
longer-prefixes	(Optional) Displays the specified route and all more-specific routes.
injected	(Optional) Displays more-specific prefixes injected into the BGP routing table.
shorter-prefixes	(Optional) Displays the specified route and all less-specific routes.
length	(Optional) The prefix length. The range is a number from 0 to 32.
bestpath	(Optional) Displays the best path for this prefix.
best-path-reason	(Optional) Displays the reason why a path loses to the bestpath. **Note** If the best-path is yet to be selected, then the output will be "Best Path Evaluation: No best path"
multipaths	(Optional) Displays multipaths for this prefix.
subnets	(Optional) Displays the subnet routes for the specified prefix.
all	(Optional) Displays all address family information in the BGP routing table.
oer-paths	(Optional) Displays Optimized Edge Routing (OER) controlled prefixes in the BGP routing table.
prefix-list *name*	(Optional) Filters the output based on the specified prefix list.
pending-prefixes	(Optional) Displays prefixes that are pending deletion from the BGP routing table.
route-map *name*	(Optional) Filters the output based on the specified route map.
version *version-number*	(Optional) Displays all prefixes with network versions greater than or equal to the specified version number. The range is from 1 to 4294967295.
recent *offset-value*	(Optional) Displays the offset from the current routing table version. The range is from 1 to 4294967295.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was modified. The display of prefix advertisement statistics was added.
12.0(6)T	This command was modified. The display of a message indicating support for route refresh capability was added.
12.0(14)ST	This command was modified. The **prefix-list**, **route-map**, and **shorter-prefixes** keywords were added.
12.2(2)T	This command was modified. The output was modified to display multipaths and the best path to the specified network.
12.0(21)ST	This command was modified. The output was modified to show the number of Multiprotocol Label Switching (MPLS) labels that arrive at and depart from a prefix.
12.0(22)S	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.2(14)S	This command was modified. A message indicating support for BGP policy accounting was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(15)T	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.3(2)T	This command was modified. The **all** keyword was added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(8)T	This command was modified. The **oer-paths** keyword was added.
12.4(15)T	This command was modified. The **pending-prefixes**, **bestpath**, **multipaths**, and **subnets** keywords were added.
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.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.

Release	Modification
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(22)T	This command was modified. The **version** *version-number* and the **recent** *offset-value* keyword and argument pairs were added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format was changed to asplain.
12.2(33)SRE	This command was modified. The command output was modified to show the backup path and the best external path information. Support for the best external route and backup path was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.2(1)S	This command was modified to display an Resource Public Key Infrastructure (RPKI) validation code per network, if one applies.
Cisco IOS XE Release 3.5S	This command was modified to display an RPKI validation code per network, if one applies.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(4)S	This command was modified. Output about discarded or unknown path attributes was added for the BGP Attribute Filter feature. Output about additional path selection was added for the BGP Additional Paths feature. Output about paths imported from a virtual routing and forwarding (VRF) table to the global table was added for the BGP Support for IP Prefix Export from a VRF table into the global table.
Cisco IOS XE Release 3.7S	This command was modified. Output about discarded or unknown path attributes was added for the BGP Attribute Filter feature. Output about additional path selection was added for the BGP Additional Paths feature. Output about paths imported from a VRF table to the global table was added for the BGP Support for IP Prefix Export from a VRF table into the global table.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.
Cisco IOS XE Gibraltar 16.10.1	The **best-path-reason** keyword was added to this command. BGP Path Installation Timestamp was added to the ouptut of the command. BGP Peak Prefix Watermark was added to the ouptut of the command.

Usage Guidelines

The **show ip bgp** command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

When changes are made to the network address, the network version number is incremented. Use the **version** keyword to view a specific network version.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

oer-paths Keyword

In Cisco IOS Release 12.3(8)T and later releases, BGP prefixes that are monitored and controlled by OER are displayed by entering the **show ip bgp** command with the **oer-paths** keyword.

show ip bgp: Example

The following sample output displays the BGP routing table:

```
Device# show ip bgp

BGP table version is 6, local router ID is 10.0.96.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop            Metric LocPrf Weight  Path

N*   10.0.0.1          10.0.0.3                 0             0  3 ?

N*>                    10.0.3.5                 0             0  4 ?

Nr   10.0.0.0/8        10.0.0.3                 0             0  3 ?

Nr>                    10.0.3.5                 0             0  4 ?

Nr>  10.0.0.0/24       10.0.0.3                 0             0  3 ?

V*>  10.0.2.0/24       0.0.0.0                  0         32768  i

Vr>  10.0.3.0/24       10.0.3.5                 0             0  4 ?
```

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

Table 27: show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry is a RIB-failure. • S—The table entry is stale. • m—The table entry has multipath to use for that network. • b—The table entry has a backup path to use for that network. • x—The table entry has a best external route to use for the network.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • a—Path is selected as an additional path. • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
RPKI validation codes	If shown, the RPKI validation state for the network prefix, which is downloaded from the RPKI server. The codes are shown only if the **bgp rpki server** or **neighbor announce rpki state** command is configured.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
(stale)	Indicates that the following path for the specified autonomous system is marked as "stale" during a graceful restart process.
Updated On	The time at which the path is received or updated.

show ip bgp (4-Byte Autonomous System Numbers): Example

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Device# show ip bgp

BGP table version is 4, local router ID is 172.16.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
```

show ip bgp network: Example

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```
Device# show ip bgp 192.168.1.0

BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```
Device# show ip bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
```

```
Advertised to update-groups:
   1
200
  10.71.8.165 from 10.71.8.165 (192.168.0.102)
    Origin incomplete, localpref 100, valid, external, backup/repair
    Only allowed to recurse through connected route
200
  10.71.11.165 from 10.71.11.165 (192.168.0.102)
    Origin incomplete, localpref 100, weight 100, valid, external, best
    Only allowed to recurse through connected route
200
  10.71.10.165 from 10.71.10.165 (192.168.0.104)
    Origin incomplete, localpref 100, valid, external,
    Only allowed to recurse through connected route
```

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

Table 28: show ip bgp ip-address Field Descriptions

Field	Description
BGP routing table entry for	IP address or network number of the routing table entry.
version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	The number of available paths, and the number of installed best paths. This line displays "Default-IP-Routing-Table" when the best path is installed in the IP routing table.
Multipath	This field is displayed when multipath load sharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.
Advertised to update-groups	The number of each update group for which advertisements are processed.
Origin	Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).
Extended Community	This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.

show ip bgp all: Example

The following is sample output from the **show ip bgp** command entered with the **all** keyword. Information about all configured address families is displayed.

```
Device# show ip bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
For address family: VPNv4 Unicast   *****
BGP table version is 21, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
*> 10.1.1.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.2.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.3.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.4.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.5.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*>i172.17.1.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.2.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.3.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.4.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.5.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
For address family: IPv4 Multicast   *****
BGP table version is 11, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.40.40.0/26    172.16.14.110         2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1              1622             0 15 20 1 {2} e
*> 10.40.40.64/26   172.16.14.110         2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1              1622             0 15 20 1 {2} e
*> 10.40.40.128/26  172.16.14.110         2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1              2563             0 15 20 1 {2} e
*> 10.40.40.192/26  10.1.1.1              2563             0 15 20 1 {2} e
*> 10.40.41.0/26    10.1.1.1              1209             0 15 20 1 {2} e
*>i10.102.0.0/16    10.1.1.1               300    500      0 5  4 {101,102} e
*>i10.103.0.0/16    10.1.1.1               300    500      0 5  4 {101,102} e
For address family: NSAP Unicast *****
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network                      Next Hop                Metric LocPrf Weight Path
* i45.0000.0002.0001.000c.00     49.0001.0000.0000.0a00                100      0 ?
* i46.0001.0000.0000.0000.0a00   49.0001.0000.0000.0a00                100      0 ?
* i47.0001.0000.0000.000b.00     49.0001.0000.0000.0a00                100      0 ?
* i47.0001.0000.0000.000e.00     49.0001.0000.0000.0a00
```

show ip bgp longer-prefixes: Example

The following is sample output from the **show ip bgp longer-prefixes** command:

```
Device# show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.1.0         10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.11.0        10.92.72.30        42482         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.14.0        10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.15.0        10.92.72.30         8696         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.16.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.17.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.18.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.19.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
```

show ip bgp shorter-prefixes: Example

The following is sample output from the **show ip bgp shorter-prefixes** command. An 8-bit prefix length is specified.

```
Device# show ip bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2               0               0 200 ?
```

show ip bgp prefix-list: Example

The following is sample output from the **show ip bgp prefix-list** command:

```
Device# show ip bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
```

```
*                   10.0.0.2                 0             0 200 ?
```

show ip bgp route-map: Example

The following is sample output from the **show ip bgp route-map** command:

```
Device# show ip bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                 0           0 200 ?
```

show ip bgp (Additional Paths): Example

The following output indicates (for each neighbor) whether any of the additional path tags (group-best, all, best 2 or best 3) are applied to the path. A line of output indicates rx pathid (received from neighbor) and tx pathid (announcing to neighbors). Note that the "Path advertised to update-groups:" is now per-path when the BGP Additional Paths feature is enabled.

```
Device# show ip bgp 10.0.0.1 255.255.255.224

BGP routing table entry for 10.0.0.1/28, version 82
Paths: (10 available, best #5, table default)
  Path advertised to update-groups:
     21         25
  Refresh Epoch 1
  20 50, (Received from a RR-client)
    192.0.2.1 from 192.0.2.1 (192.0.2.1)
      Origin IGP, metric 200, localpref 100, valid, internal, all
      Originator: 192.0.2.1, Cluster list: 2.2.2.2
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x9
      Updated on Aug 14 2018 18:30:39 PST
  Path advertised to update-groups:
     18         21
  Refresh Epoch 1
  30
    192.0.2.2 from 192.0.2.2 (192.0.2.2)
      Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
      Originator: 192.0.2.2, Cluster list: 4.4.4.4
      mpls labels in/out 16/nolabel
      rx pathid: 0x1, tx pathid: 0x8
      Updated on Aug 14 2018 18:30:39 PST
  Path advertised to update-groups:
     16         18         19         20         21         22         24
     25         27
  Refresh Epoch 1
  10
    192.0.2.3 from 192.0.2.3 (192.0.2.3)
      Origin IGP, metric 200, localpref 100, valid, external, best2, all
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x7
      Updated on Aug 14 2018 18:30:39 PST
  Path advertised to update-groups:
     20         21         22         24         25
  Refresh Epoch 1
```

```
10
  192.0.2.4 from 192.0.2.4 (192.0.2.4)
    Origin IGP, metric 300, localpref 100, valid, external, best3, all
    mpls labels in/out 16/nolabel
    rx pathid: 0, tx pathid: 0x6
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
   10         13         17         18         19         20         21
   22         23         24         25         26         27         28
Refresh Epoch 1
10
  192.0.2.5 from 192.0.2.5 (192.0.2.5)
    Origin IGP, metric 100, localpref 100, valid, external, best
    mpls labels in/out 16/nolabel
    rx pathid: 0, tx pathid: 0x0
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
   21
Refresh Epoch 1
30
  192.0.2.6 from 192.0.2.6 (192.0.2.6)
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.6, Cluster list: 5.5.5.5
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x5
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
   18         23         24         26         28
Refresh Epoch 1
60 40, (Received from a RR-client)
  192.0.2.7 from 192.0.2.7 (192.0.2.7)
    Origin IGP, metric 250, localpref 100, valid, internal, group-best
    Originator: 192.0.2.7, Cluster list: 3.3.3.3
    mpls labels in/out 16/nolabel
    rx pathid: 0x2, tx pathid: 0x2
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
   25
Refresh Epoch 1
30 40, (Received from a RR-client)
  192.0.2.8 from 192.0.2.8 (192.0.2.8)
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.8, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x3
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
   18         21         23         24         25         26         28
Refresh Epoch 1
20 40, (Received from a RR-client)
  192.0.2.9 from 192.0.2.9 (192.0.2.9)
    Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
    Originator: 192.0.2.9, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x4
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
   21
Refresh Epoch 1
30 40
  192.0.2.9 from 192.0.2.9 (192.0.2.9)
    Origin IGP, metric 100, localpref 100, valid, internal, all
    Originator: 192.0.2.9, Cluster list: 4.4.4.4
    mpls labels in/out 16/nolabel
```

```
      rx pathid: 0x1, tx pathid: 0x1
      Updated on Aug 14 2018 18:30:39 PST
```

show ip bgp network (BGP Attribute Filter): Example

The following is sample output from the **show ip bgp** command that displays unknown and discarded path attributes:

```
Device# show ip bgp 192.0.2.0/32

BGP routing table entry for 192.0.2.0/32, version 0
Paths: (1 available, no best path)
  Refresh Epoch 1
  Local
    192.168.101.2 from 192.168.101.2 (192.168.101.2)
      Origin IGP, localpref 100, valid, internal
      unknown transitive attribute: flag 0xE0 type 0x81 length 0x20
        value 0000 0000 0000 0000 0000 0000 0000 0000
              0000 0000 0000 0000 0000 0000 0000 0000

      unknown transitive attribute: flag 0xE0 type 0x83 length 0x20
        value 0000 0000 0000 0000 0000 0000 0000 0000
              0000 0000 0000 0000 0000 0000 0000 0000

      discarded unknown attribute: flag 0x40 type 0x63 length 0x64
       value 0000 0000 0000 0000 0000 0000 0000 0000
              0000 0000 0000 0000 0000 0000 0000 0000
```

show ip bgp version: Example

The following is sample output from the **show ip bgp version** command:

```
Device# show ip bgp version

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 192.168.34.2/24 10.0.0.1 0 0 1 ?
*> 192.168.35.2/24 10.0.0.1 0 0 1 ?
```

The following example shows how to display the network version:

```
Device# show ip bgp 192.168.34.2 | include version

BGP routing table entry for 192.168.34.2/24, version 5
```

The following sample output from the **show ip bgp version recent** command displays the prefix changes in the specified version:

```
Device# show ip bgp version recent 2

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf  Weight   Path
*> 192.168.134.1/28     10.0.0.1         0             0       1 ?
```

```
*> 192.168.134.19/28    10.0.0.1         0             0       1 ?
*> 192.168.134.34/28    10.0.0.1         0             0       1 ?
```

The following example shows the sample output for the **show ip bgp** *ip-address* **best-path-reason** command, listing the reason why a path loses to the best path:

```
Device# show ip bgp 80.230.70.96 best-path-reason

BGP routing table entry for 192.168.3.0/24, version 72
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
    2
  Refresh Epoch 1
2
  10.0.101.1 from 10.0.101.1 (10.0.101.1)
    Origin IGP, localpref 100, valid, external
    Extended Community: RT:100:100
    rx pathid: 0, tx pathid: 0
    Updated on Aug 14 2018 18:34:12 PST
    Best Path Evaluation: Path is younger
Refresh Epoch 1
1
  10.0.96.254 from 10.0.96.254 (10.0.96.254)
  Origin IGP, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: 0x0
  Updated on Aug 14 2018 18:30:39 PST
  Best Path Evaluation: Overall best path
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets BGP connections using hard or soft reconfiguration.
ip bgp community new-format	Configures BGP to display communities in the format AA:NN.
ip prefix-list	Creates a prefix list or adds a prefix-list entry.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol.
router bgp	Configures the BGP routing process.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

show ip bgp [{**ipv4** {**multicast** | **unicast**} | **vpnv4 all** | **vpnv6 unicast all**}] **neighbors** [{**slow** *ip-address* | *ipv6-address* [{**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**}] | **include Fall over** }]

Syntax Description

ipv4	(Optional) Displays peers in the IPv4 address family.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
unicast	(Optional) Specifies IPv4 unicast address prefixes.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
slow	(Optional) Displays information about dynamically configured slow peers.
ip-address	(Optional) IP address of the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
ipv6-address	(Optional) IP address of the IPv6 neighbor.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to this neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.

include Fall over	(Optional) Displays all fallover with maximum-metric that is configured for the neighbor.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Mainline and T Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The **received-routes** keyword was added.
12.2(4)T	This command was modified. The **received** and **prefix-filter** keywords were added.
12.2(15)T	This command was modified. Support for the display of BGP graceful restart capability information was added.
12.3(7)T	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.4(4)T	This command was modified. Support for the display of Bidirectional Forwarding Detection (BFD) information was added.
12.4(11)T	This command was modified. Support for the **policy** and **detail** keywords was added.
12.4(20)T	This command was modified. The output was modified to support BGP TCP path MTU discovery.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.

S Release	Modification
12.0(18)S	This command was modifed. The output was modified to display the no-prepend configuration option.
12.0(21)ST	This command was modifed. The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	This command was modified. Support for the display of BGP graceful restart capability information was added. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.0(25)S	This command was modified. The **policy** and **detail** keywords were added.
12.0(27)S	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.

S Release	Modification
12.0(31)S	This command was modified. Support for the display of BFD information was added.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(18)SXE	This command was modified. Support for the display of BFD information 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 modified. The output was modified to support BGP TCP path Maximum Transmission Unit (MTU) discovery.
12.2(33)SRB	This command was modified. Support for the **policy** and **detail** keywords was added.
12.2(33)SXH	This command was modified. Support for displaying BGP dynamic neighbor information was added.
12.2(33)SRC	This command was modified. Support for displaying BGP graceful restart information was added.
12.2(33)SB	This command was modified. Support for displaying BFD and the BGP graceful restart per peer information was added, and support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)SRE	This command was modified. Support for displaying BGP best external and BGP additional path features information was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)S	This command was modified. The Layer 2 VPN address family is displayed if graceful restart or nonstop forwarding (NSF) is enabled.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.

S Release	Modification
15.2(4)S	This command was modified and implemented on the Cisco 7200 series router. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Cisco IOS XE	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.1S	This command was modified. The **slow** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. Support for displaying BGP BFD multihop and C-bit information was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
Cisco IOS XE Release 3.8S	This command was modified. In support of the BGP Multi-Cluster ID feature, the cluster ID of a neighbor is displayed if the neighbor is assigned a cluster.
Cisco IOS XE Gibraltar 16.10.1	BGP Peak Prefix Watermark was added to the command output.
Cisco IOS XE Release 17.1.1	This command was modified. The **include Fall over** keyword was added.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses

asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Later Releases

When BGP neighbors use multiple levels of peer templates, determining which policies are applied to the neighbor can be difficult.

In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer group or a peer policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections.

show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
```

```
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 29: show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when a network administrator is migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors; “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.

Field	Description
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
last write	Time, in hh:mm:ss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. "advertised and received" is displayed when a capability is successfully exchanged between two routers.
Route refresh	Status of the route refresh capability.
MPLS Label capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Revd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.

Field	Description
For address family:	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
1 update-group member	Number of the update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes Current	Number of prefixes accepted for this address family.
Prefixes Total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that a prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as best paths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS_PATH length policy denials.
* AS_PATH loop	Displays outbound AS_PATH loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system 0.

Field	Description
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound nonlocal next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress map.
* advertise-map	Displays inbound denials due to an advertise map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the best path came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the best path came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a customer edge (CE) router.
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Current session network count peaked...	Displays the peak number of networks observed in the current session.
Highest network count observed at...	Displays the peak number of networks observed since startup.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP time to live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.

Field	Description
unread input bytes	Number of bytes of packets still to be processed.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number of times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is higher than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.

Field	Description
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Shortest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Longest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
out of order:	Number of packets received out of sequence.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).
Second Congestion	Number of second retransmissions sent due to congestion.

show ip bgp neighbors (4-Byte Autonomous System Numbers)

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp neighbors

BGP neighbor is 192.168.1.2,  remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
```

```
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
.
.
.
BGP neighbor is 192.168.3.2,  remote AS 65550, external link
 Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
```

show ip bgp neighbors advertised-routes

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Device# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

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

Table 30: show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the interautonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp neighbors check-control-plane-failure

The following is sample output from the **show ip bgp neighbors** command entered with the **check-control-plane-failure** option configured:

```
Device# show ip bgp neighbors 10.10.10.1

BGP neighbor is 10.10.10.1,  remote AS 10, internal link
 Fall over configured for session
 BFD is configured. BFD peer is Up. Using BFD to detect fast fallover (single-hop) with
c-bit check-control-plane-failure.
 Inherits from template cbit-tps for session parameters
  BGP version 4, remote router ID 10.7.7.7
  BGP state = Established, up for 00:03:55
  Last read 00:00:02, last write 00:00:21, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
```

show ip bgp neighbors paths

The following is sample output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Device# show ip bgp neighbors 172.29.232.178 paths 10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

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

Table 31: show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

show ip bgp neighbors received prefix-filter

The following example shows that a prefix list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Device# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

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

Table 32: show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

show ip bgp neighbors policy

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer group or a peer-policy template.

```
Device# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

Cisco IOS Release 12.0(31)S, 12.4(4)T, 12.2(18)SXE, and 12.2(33)SB

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast fallover for the BGP neighbor that is a BFD peer:

```
Device# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
.
.
.
 Using BFD to detect fast fallover
```

Cisco IOS Release 12.2(33)SRA and 12.4(20)T

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
Device# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Cisco IOS Release 12.2(33)SXH

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group group192 and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created:

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB

The following is partial output from the **show ip bgp neighbors** command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
```

```
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

Cisco IOS Release 15.1(1)S: Example

The following is partial output from the **show ip bgp neighbors** command. For this release, the display includes the Layer 2 VFN address family information if graceful restart or NSF is enabled.

```
Device# show ip bgp neighbors

Load for five secs: 2%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:49:17.034 GMT Wed Sep 22 2010
BGP neighbor is 10.1.1.3,  remote AS 2, internal link
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:14:32
  Last read 00:00:30, last write 00:00:43, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family L2VPN Vpls: advertised and received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
      Address families advertised by peer:
        IPv4 Unicast (was not preserved), L2VPN Vpls (was not preserved)
    Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                4         16
    Keepalives:            16         16
    Route Refresh:          0          0
    Total:                 21         33
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
  Session: 10.1.1.3
  BGP table version 34, neighbor version 34/0
  Output queue size : 0
  Index 1, Advertise bit 0
  1 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             2         11 (Consumes 572 bytes)
    Prefixes Total:               4         19
    Implicit Withdraw:            2          6
    Explicit Withdraw:            0          2
```

```
    Used as bestpath:             n/a          7
    Used as multipath:            n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    NEXT_HOP is us:                     n/a          1
    Bestpath from this peer:             20        n/a
    Bestpath from iBGP peer:              8        n/a
    Invalid Path:                        10        n/a
    Total:                               38          1
  Number of NLRIs in the update sent: max 2, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
 For address family: L2VPN Vpls
  Session: 10.1.1.3
  BGP table version 8, neighbor version 8/0
  Output queue size : 0
  Index 1, Advertise bit 0
  1 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              1          1 (Consumes 68 bytes)
    Prefixes Total:                2          1
    Implicit Withdraw:             1          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          1
    Used as multipath:           n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Bestpath from this peer:              4        n/a
    Bestpath from iBGP peer:              1        n/a
    Invalid Path:                         2        n/a
    Total:                                7          0
  Number of NLRIs in the update sent: max 1, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Address tracking is enabled, the RIB does have a route to 10.1.1.3
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 seconds
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 255
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.3, Foreign port: 48485
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0xE750C):
Timer          Starts    Wakeups            Next
Retrans            18          0             0x0
TimeWait            0          0             0x0
AckHold            22         20             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 3196633674  snduna: 3196634254  sndnxt: 3196634254     sndwnd:  15805
irs: 1633793063  rcvnxt: 1633794411  rcvwnd:      15037  delrcvwnd:   1347
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 2 ms, maxRTT: 300 ms, ACK hold: 200 ms
```

```
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
Datagrams (max data segment is 1436 bytes):
Rcvd: 42 (out of order: 0), with data: 24, total data bytes: 1347
Sent: 40 (retransmit: 0 fastretransmit: 0),with data: 19, total data bytes: 579
```

BGP Attribute Filter and Enhanced Attribute Error Handling

The following is sample output from the **show ip bgp neighbors** command that indicates the discard attribute values and treat-as-withdraw attribute values configured. It also provides a count of received Updates matching a treat-as-withdraw attribute, a count of received Updates matching a discard attribute, and a count of received malformed Updates that are treat-as-withdraw.

```
Device# show ip bgp vpnv4 all neighbors 10.0.103.1

BGP neighbor is 10.0.103.1,  remote AS 100, internal link
 Path-attribute treat-as-withdraw inbound
 Path-attribute treat-as-withdraw value 128
 Path-attribute treat-as-withdraw 128 in: count 2
 Path-attribute discard 128 inbound
 Path-attribute discard 128 in: count 2

       Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    MALFORM treat as withdraw:            0          1
    Total:                                0          1
```

BGP Additional Paths

The following output indicates that the neighbor is capable of advertising additional paths and sending additional paths it receives. It is also capable of receiving additional paths and advertised paths.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds

  Neighbor capabilities:
    Additional paths Send: advertised and received
    Additional paths Receive: advertised and received
    Route refresh: advertised and received(old & new)
    Graceful Restart Capabilty: advertised and received
    Address family IPv4 Unicast: advertised and received
```

BGP—Multiple Cluster IDs

In the following output, the cluster ID of the neighbor is displayed. (The vertical bar and letter “i” for “include” cause the device to display only lines that include the user's input after the “i”, in this case, “cluster-id.”) The cluster ID displayed is the one directly configured through a neighbor or a template.

```
Device# show ip bgp neighbors 192.168.2.2 | i cluster-id
```

```
 Configured with the cluster-id 192.168.15.6
```

BGP Peak Prefix Watermark

The following sample output shows the peak watermarks and their timestamps displayed for the peak number of route entries per neighbor bases:

```
Device# show ip bgp ipv4 unicast neighbors 11.11.11.11

BGP neighbor is 11.11.11.11, remote AS 1, internal link
BGP version 4, remote router ID 0.0.0.0
BGP state = Idle, down for 00:01:43
Neighbor sessions:
0 active, is not multisession capable (disabled)
Stateful switchover support enabled: NO
Do log neighbor state changes (via global configuration)
Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
BGP table version 27, neighbor version 1/27
Output queue size : 0
Index 0, Advertise bit 0

Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
    Sent Rcvd
Prefix activity:      ---- ----
 Prefixes Current:              0    0
 Prefixes Total:                0    0
 Implicit Withdraw:             0    0
 Explicit Withdraw:             0    0
 Used as bestpath:            n/a    0
 Used as multipath:           n/a    0
 Used as secondary:           n/a    0
                              Outbound Inbound
Local Policy Denied Prefixes: -------- -------
 Total:                                0       0
Number of NLRIs in the update sent: max 2, min 0
Current session network count peaked at 20 entries at 00:00:23 Aug 8 2018 PST (00:01:29.156
ago).
Highest network count observed at 20 entries at 23:55:32 Aug 7 2018 PST (00:06:20.156
ago).
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
Refresh Epoch: 1
Last Sent Refresh Start-of-rib: never
Last Sent Refresh End-of-rib: never
Last Received Refresh Start-of-rib: never
Last Received Refresh End-of-rib: never
                                  Sent Rcvd
Refresh activity:                 ---- ----
 Refresh Start-of-RIB                1    0
 Refresh End-of-RIB                  0    0
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.

Command	Description
bgp enhanced-error	Restores the default behavior of treating Update messages that have a malformed attribute as withdrawn, or includes iBGP peers in the Enhanced Attribute Error Handling feature.
neighbor path-attribute discard	Configures the device to discard unwanted Update messages from the specified neighbor that contain a specified path attribute.
neighbor path-attribute treat-as-withdraw	Configures the device to withdraw from the specified neighbor unwanted Update messages that contain a specified attribute.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
router bgp	Configures the BGP routing process.

show ip bgp vpnv4

To display VPN Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [{[{*ip-prefix*/*length* [{*mask* | **bestpath** | **multipaths**}] | *network-address* [{*mask* | **bestpath** | **longer-prefixes** | **multipaths** | **shorter-prefixes** | **subnets**}]}] | **cidr-only** | **cluster-ids** | **community** | **community-list** | **dampening** | **extcommunity-list** *extcommunity-list-name* | **filter-list** | **inconsistency nexthop-label** | **inconsistent-as** | **labels** | **neighbors** [{{*ip-addressipv6-address*} [{**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** | **policy** [**detail**] | **received** | **received-routes** | **routes**}] | **slow**}] | **nexthops** | **oer-paths** | **path-attribute** {**discard** | **unknown**} | **paths** [*line*] | **peer-group** | **pending-prefixes** | **prefix-list** *prefix-list-name* | **quote-regexp** | **regexp** | **replication** [*update-group-index*] [*update-group-member-address*] | **rib-failure** | **route-map** *route-map-name* | **summary** | **update-group** | **update-source** | **version** {*version-number* | **recent** *offset-value*}}]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
ip-prefix/length	(Optional) IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
network-address	(Optional) IP address of a network in the BGP routing table.
mask	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful netmasks.
cluster-ids	(Optional) Displays configured cluster IDs.
community	(Optional) Displays routes that match this community.
community-list	(Optional) Displays routes that match this community list.
dampening	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list *extended-community-list-name*	(Optional) Displays routes that match the extended community list.
filter-list	(Optional) Displays routes that conform to the filter list.
inconsistency nexthop-label	(Optional) Displays all inconsistent paths.

inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
ip-address	(Optional) Displays information about the neighbor at this IPv4 address.
ipv6-address	(Optional) Displays information about the neighbor at this IPv6 address.
advertised-routes	(Optional) Displays advertised routes from the specified neighbor.
dampened-routes	(Optional) Displays dampened routes from the specified neighbor.
flap-statistics	(Optional) Displays flap statistics about the specified neighbor.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
policy [detail]	(Optional) Displays configured policies for the specified neighbor.
slow	(Optional) Displays BGP slow peer information.
nexthops	(Optional) Displays nexthop address table.
oer-paths	(Optional) Displays all OER-controlled paths.
path-attribute	(Optional) Displays path-attribute-specific information.
discard	(Optional) Displays prefixes with discarded path attribute.
unknown	(Optional) Displays prefixes with unknown path attribute.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
pending-prefixes	(Optional) Displays prefixes that are pending deletion.
prefix-list *prefix-list*	(Optional) Displays routes that match the prefix list.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.
replication	(Optional) Displays replication status of update group(s).

rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
route-map	(Optional) Displays routes that match the route map.
summary	(Optional) Displays BGP neighbor status.
update-group	(Optional) Displays information on update groups.
update-source	(Optional) Displays update source interface table.
version	(Optional) Displays prefixes with matching version numbers.
version-number	(Optional) If the **version** keyword is specified, either a *version-number* or the **recent** keyword and an *offset-value* are required.
recent *offset-value*	(Optional) Displays prefixes with matching version numbers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. The output of the **show ip bgp vpnv4 all** *ip-prefix* command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	This command was modified. The **tags** keyword was replaced by the **labels** keyword to conform to the MPLS guidelines.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(27)S	This command was modified. The output of the **show ip bgp vpnv4 all labels** command was enhanced to display explicit-null label information.
12.3	This command was modified. The **rib-failure** keyword was added for VRFs.
12.2(22)S	This command was modified. The output of the **show ip bgp vpnv4 vrf** *vrf-name* **labels** command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP nonstop routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.

Release	Modification
12.2(33)SRA	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
12.2(33)SXH	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID. **Note** In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby Route Processor in NSF/SSO mode.
12.4(20)T	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
15.0(1)M	This command was modified. The output was modified to support the BGP Event-Based VPN Import feature.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP Event-Based VPN Import, BGP best external, and BGP additional path features.
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.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was implemented on the Cisco 7200 series router and the output was modified to display unknown attributes and discarded attributes associated with a prefix.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified to display unknown attributes and discarded attributes associated with a prefix.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all
```

```
BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32       10.0.0.21               11    100      0 ?
*> 10.7.7.7/32       10.150.0.2              11         32768 ?
*>i10.69.0.0/30      10.0.0.21                0    100      0 ?
*> 10.150.0.0/24     0.0.0.0                  0         32768 ?
```

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

Table 33: show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

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

Table 34: show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

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

Table 35: show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Router# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nolabel/17
  100, imported path from 300:1:192.168.9.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
```

```
mpls labels in/out nolabel/17
```

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

Table 36: show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is internal if the path is learned via iBGP. The field is external if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

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

Table 37: show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Note In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affects the output of this command on the standby Route Processor (RP). In Cisco IOS Release 12.2(33)SXH, the standby RP does not display any output from the **show ip bgp vpnv4** command.

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
```

```
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32  0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)


Router# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

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

Table 38: show ip bgp vpnv4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Router# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24       10.0.0.0        19/aggregate(v1)
   10.0.0.1/32       10.0.0.0        20/nolabel
   10.1.1.1/32       10.0.0.0        21/aggregate(v1)
   10.10.10.10/32    10.0.0.1        25/exp-null

   10.168.100.100/32
                     10.0.0.1        23/exp-null
   10.168.101.101/32
```

```
                    10.0.0.1         22/exp-null
```

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

Table 39: show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(31)SB2, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, Cisco IOS XE Release 2.1, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

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

Table 40: show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

In the following example, the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the best path or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Router# show ip bgp vpnv4 all 172.17.0.0
```

```
BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

In the following example, BGP Event-Based VPN Import feature configuration information is shown for Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the Route Targets (RT) imported by the specified VRF. In this situation, the imported path is marked as "not-in-vrf" as shown in the output. Note that on the net for vrf-A, this path is not the best path because any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
mpls labels in/out nolabel/16
```

In the following example, the unknown attributes and discarded attributes associated with the prefix are displayed.

```
Device# show ip bgp vpnv4 all 10.0.0.0/8

BGP routing table entry for 100:200:10.0.0.0/8, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    10.0.103.1 from 10.0.103.1 (10.0.103.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:100
      Connector Attribute: count=1
       type 1 len 12 value 22:22:10.0.101.22
      mpls labels in/out nolabel/16
      unknown transitive attribute: flag E0 type 129 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 140 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 120 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

```
      discarded unknown attribute: flag C0 type 128 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

The following example is based on the BGP—VPN Distinguisher Attribute feature. The output displays an Extended Community attribute, which is the VPN distinguisher (VD) of 104:1.

```
Device# show ip bgp vpnv4 unicast all 1.4.1.0/24

BGP routing table entry for 104:1:1.4.1.0/24, version 28
Paths: (1 available, best #1, no table)
   Advertised to update-groups:
      1
   Refresh Epoch 1
   1001
     19.0.101.1 from 19.0.101.1 (19.0.101.1)
       Origin IGP, localpref 100, valid, external, best
       Extended Community: VD:104:1
       mpls labels in/out nolabel/16
       rx pathid: 0, tx pathid: 0x0
```

The following example includes “allow-policy” in the output, indicating that the BGP—Support for iBGP Local-AS feature was configured for the specified neighbor by configuring the **neighbor allow-policy** command.

```
Device# show ip bgp vpnv4 all neighbors 192.168.3.3 policy

Neighbor: 192.168.3.3, Address-Family: VPNv4 Unicast
Locally configured policies:
 route-map pe33 out
 route-reflector-client
 allow-policy
 send-community both
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
neighbor allow-policy	Allows iBGP policies to be configured for the specified neighbor.
set extcommunity vpn-distinguisher	Sets a VPN distinguisher attribute to routes that pass a route map.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show redundancy config-sync

To display failure information generated during a bulk synchronization from the active Performance Routing Engine (PRE) to the standby PRE, use the **show redundancy config-sync** command in user EXEC or privileged EXEC modes.

show redundancy config-sync

Syntax Description

failures	Displays failures related to bulk synchronisation of the standby PRE.
bem	Displays Best Effort Method (BEM) failure list.
mcl	Displays Mismatched Command List (MCL) failure list.
prc	Displays Parser Return Code (PRC) failure list.
ignored failures mcl	Displays mismatched commands in the MCL that are ignored.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

This command is used on the active PRE only.

If there are mismatched commands between the active and standby PRE, remove the configuration lines that are not supported on the standby image. If it is not possible to remove the mismatched lines, or it has been determined that the mismatched lines are not critical to the operation of the system, use the command **redundancy config-sync ignore mismatched-commands** to temporarily ignore them.

Examples

The following example displays a mismatched command list:

```
Device# show redundancy config-sync failures mcl
Mismatched Command List
-----------------------
- tacacs-server host 209.165.200.225 timeout 5
```

The following example shows that no mismatched commands are ignored:

```
router# show redundancy config-sync ignored failures mcl
Ignored Mismatched Command List
-------------------------------
The list is empty
```

The following example displays a Parser Return Code failure list:

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------
router bgp 999
```

```
address-family ipv4 vrf TEST2
- bgp dampening 44 66 66 44
!  "address-family"
address-family ipv4 vrf TEST1
- bgp dampening 44 66 66 44
!  "address-family"
```

The following example displays a Best Effort Method failure list:

```
Device# show redundancy config-sync failures bem
BEM Failed Command List
-----------------------
interface Tunnel0
- tunnel mpls traffic-eng priority 7 7
!  "interface"
- next-address loose 10.165.202.158
- next-address loose 10.165.202.129
```

Related Commands

Command	Description
redundancy force-switchover	Forces the standby PRE to assume the role of the active PRE.
show redundancy	Displays current active and standby PRE redundancy status.
show redundancy platform	Displays active and standby PRE and software information.

show redundancy config-sync ignored failures mcl

To display failure information generated during a bulk synchronization of commands from an active Route Processor (RP) module to a standby RP module, use the **show redundancy config-sync ignored failures mcl** command in user EXEC or privileged EXEC modes.

show redundancy config-sync ignored failures mcl

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command is used on the active RP module only.

If there are mismatched commands between active and standby RP modules, remove configuration lines that are not supported on the standby RP module. If it is not possible to remove mismatched lines, or if mismatched lines are not critical to the operation of the system, use the **redundancy config-sync ignore mismatched-commands** command to temporarily ignore them.

Examples

The following is sample output from the **show redundancy config-sync ignored failures mcl** command when there are no mismatched commands:

```
Device# show redundancy config-sync ignored failures mcl

Ignored Mismatched Command List
-------------------------------
The list is empty
```

The following is sample output from the **show redundancy config-sync ignored failures mcl** command. It shows the list of commands that are ignored:

```
Device# show redundancy config-sync ignored failures mcl

Mismatched Command List
-----------------------
interface Multilink0
! <submode> "interface"
- multilink-group 0
! </submode> "interface"
interface GigabitEthernet1/1
! <submode> "interface"
- ip rtp priority 2000 0
 ! </submode> "interface"
router isis
! <submode> "router"
- exit-address-family
```

```
! </submode> "router"
```

Related Commands

Command	Description
redundancy force-switchover	Forces the standby RP module to assume the role of the active RP module.
show redundancy	Displays the redundancy status of the current active and standby RP modules.
show redundancy platform	Displays active and standby RP modules and software information.

standby initialization delay

To configure the standby Route Processor (RP) initialization delay, use the **standby initialization delay** command in main-CPU redundancy configuration mode. To disable the standby RP initialization delay configuration, use the **no** form of this command.

standby initialization delay *seconds* [**boot-only**]
no standby initialization delay *seconds* [**boot-only**]

Syntax Description

seconds	Duration of the standby RP initialization delay. The range is from 30 to 1800.
boot-only	(Optional) Specifies that the standby RP initialization is delayed only when the system boots up.

Command Default

The standby RP initialization delay is not configured.

Command Modes

Main-CPU redundancy configuration (config-r-mc)

Command History

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

Usage Guidelines

If the **boot-only** is used, standby RP initialization is delayed only when the system boots up. If **boot-only** is not used, standby RP initialization will be delayed when the system boots up and also after an RP switchover.

Examples

The following example shows how to configure a standby RP initialization delay of 60 seconds:

```
Device> enable
Device# configure terminal
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby initialization delay 60 boot-only
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces the standby RP to assume the role of the active RP.

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

alphanumeric	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 the 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 limit** {**cpu** *percent* **delay** *seconds* [**allow** *sessions*] | **time** *seconds*} | **dynamic limit** {**cpu** *percent* **delay** *seconds* | [**allow** *sessions*] | **periodic-update interval** [*minutes*]} | **delay** *seconds* | **rate** *sessions seconds* | **disable**}
no subscriber redundancy {**bulk limit** {**cpu** | **time**} | **dynamic limit** {**cpu** | **periodic-update interval** [*minutes*]} | **delay** | **rate** | **disable**}

Syntax Description

bulk	Configures a bulk synchronization redundancy policy.
limit	Specifies the synchronization limit.
dynamic	Configures a dynamic synchronization redundancy policy.
cpu *percent*	Specifies, in percent, the CPU busy threshold value. Range: 1 to 100. Default: 90.
delay *seconds*	Specifies the minimum time, in seconds, for a session to be ready before bulk or dynamic synchronization occurs. Range: 1 to 33550.
allow *sessions*	(Optional) Specifies the minimum number of sessions to synchronize when the CPU busy threshold is exceeded and the specified delay is met. Range: 1 to 2147483637. Default: 25.
time *seconds*	Specifies the maximum time, in seconds, for bulk synchronization to finish. Range: 1 to 3000.
periodic-update interval	Enables the periodic update of accounting statistics for subscriber sessions.
minutes	(Optional) Interval, in minutes, for the periodic update. Range: 10 to 1044. Default: 15.
rate *sessions seconds*	Specifies the number of sessions per time period for bulk and dynamic synchronization. • *sessions*—Range: 1 to 32000. Default: 250. • *seconds*—Range: 1 to 33550. Default: 1.
disable	Disables stateful switchover (SSO) for all subscriber sessions.

Command Default

The default subscriber redundancy policy is applied.

Command Modes

Global configuration (config)

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.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
Cisco IOS XE Release 3.5S	This command was modified. The **periodic-update interval** keyword and *minutes* argument were added.
15.2(1)S	This command was modified. The **disable** keyword was added.

Usage Guidelines

Cisco IOS HA functionality for broadband protocols and applications allows for SSO and In-Service Software Upgrade (ISSU) features that minimize planned and unplanned downtime and failures. HA uses the cluster control manager (CCM) to manage the capability to synchronize subscriber session initiation on the standby processor of a redundant processor system.

- Use the **bulk** keyword to create and modify the redundancy policy used during bulk (startup) synchronization.
- Use the **dynamic** keyword with the **limit** keyword to tune subscriber redundancy policies that throttle dynamic synchronization by monitoring CPU usage and synchronization rates.
- Use the **delay** keyword to establish the minimum session duration for synchronization and to manage dynamic synchronization of short-duration calls.
- Use the **rate** keyword to throttle the number of sessions to be synchronized per period.
- Use the **dynamic** keyword with the **periodic-update interval** keyword to enable subscriber sessions to periodically synchronize their dynamic accounting statistics (counters) on the standby processor. The periodic update applies to new and existing subscriber sessions. All subscriber sessions do not synchronize their data at exactly the same time. Session synchronization is spread out based on the session creation time and other factors. This command is rejected if a previous instance of the command has not finished processing.
- Use the **disable** keyword to disable SSO for all subscriber sessions.

Examples

The following example shows how to configure 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 the CPU usage:

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

The following example shows how to configure a maximum time of 90 seconds for bulk synchronization to be completed:

```
Router(config)# subscriber redundancy bulk limit time 90
```

The following example shows how to configure a 15-second delay when CPU usage exceeds 90 percent during dynamic synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy dynamic limit cpu 90 delay 15 allow 25
```

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

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

The following example shows how to configure a periodic update so that subscriber sessions synchronize their accounting statistics every 30 minutes:

```
Router(config)# subscriber redundancy dynamic periodic-update interval 30
```

The following example shows how to disable SSO for all subscriber sessions:

```
Router(config)# subscriber redundancy disable
```

Related Commands

Command	Description
show ccm sessions	Displays CCM session information.
show pppatm statistics	Displays PPPoA statistics.
show pppoe statistics	Displays PPPoE statistics.
show ppp subscriber statistics	Displays PPP subscriber 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** *hh* **:** *mm*	(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** *day hh* **:** *mm*	(Optional) Specifies the time to begin monthly Call Home messages; the valid values are as follows: • *day* is 1 to 31. • hh:mm is based on a 24-hour clock.
periodic **weekly** *day hh* **:** *mm*	(Optional) Specifies the time to begin weekly Call Home messages; the valid values are as follows: • *day* is 1 to 31. • hh:mm is based on a 24-hour clock.
diagnostic	Subscribes to diagnostic information groups.
severity *level*	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--Anetwork-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

periodic	(Optional) Specifies a periodic Call Home message, where: • **daily** *hh* **:** *mm* --Time [in 24-hour format (*hh***:***mm*)] 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 (*hh***:***mm*)] 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 (*hh***:***mm*)] 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 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.

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	(Optional) Specifies the lowest level of severity events to include in a diagnostic alert, where: • **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.
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	(Optional) Specifies the lowest level of severity events to include in an environment alert, where: • **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.
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: • **daily** *hh* **:** *mm* --Time [in 24-hour format (*hh*:*mm*)] 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 (*hh*:*mm*)] 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 (*hh*:*mm*)] 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: • **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 *match*	(Optional) Specifies a word string in the *match* 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.

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.

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.

syslog-throttling

To enable Call-Home syslog message throttling and avoid sending repetitive Call-Home syslog messages, use the **syslog-throttling** command in call home configuration mode. To disable, use the **no** form of this command.

syslog-throttling
no syslog-throttling

Syntax Description

This command has no arguments or keywords.

Command Default

Call-Home syslog message throttling is enabled.

Command Modes

Call home configuration (cfg-call-home)

Command History

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

Examples

The following example shows syslog throttling enabled in call home configuration mode:

```
Router(cfg-call-home)# syslog-throttling
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

timers nsf converge

To adjust the maximum time that a restarting router must 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 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

seconds	Time, in seconds, for which a restarting router must wait for an EOT notification. The range is from 60 to 180. The default is 120.

Command Default

The default converge timer is 120 seconds.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

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

Usage Guidelines

The **timers nsf converge** command is entered only on an NSF-capable router 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.

Note The **timers nsf converge** command is supported only on platforms that support High Availability.

Examples

The following example shows how to adjust the converge timer to 60 seconds on an NSF-capable router:

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

The following example shows how to adjust the converge timer for EIGRP IPv6 NSF:

```
Device(config)# router eigrp e1
Device(config-router)# address-family ipv6 autonomous-system 1
Device(config-router-af)# timers nsf converge 60
```

Related Commands

Command	Description
debug eigrp address-family ipv6 notifications	Displays information about EIGRP address family IPv6 event notifications.
debug eigrp nsf	Displays notifications and information about NSF events for an EIGRP routing process.
debug ip eigrp notifications	Displays information and notifications for an EIGRP routing process.
nsf (EIGRP)	Enables EIGRP NSF or EIGRP IPv6 NSF on an NSF-capable router.
show eigrp neighbors	Displays the neighbors discovered by EIGRP.
show ip protocols	Displays the parameters and the current state of the active routing protocol process.
show ipv6 protocols	Displays the parameters and the current state of the active IPv6 routing protocol process.
timers graceful-restart purge-time	Sets the graceful-restart purge-time timer to determine how long an NSF-aware router that is running EIGRP must hold routes for an inactive peer.
timers nsf signal	Sets 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

seconds	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 or address family configuration mode. To return the signal timer to the default value, use the **no** form of this command.

timers nsf signal *seconds*
no timers nsf signal

Syntax Description

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

Command Default

The default signal timer is 20 seconds.

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. Support for Address family configuration mode was added.
12.2(33)SRE	This command was modified. Support for Address family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was modified. Support for IPv6 and IPv6 VPN Routing and Forwarding (VRF) was added.
15.2(2)S	This command was modified. Support for IPv6 and IPv6 VRF was added.

Usage Guidelines

The **timers nsf signal** 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.

Note The **timers nsf signal** command is supported only on platforms that support High Availability.

Examples

The following example shows how to adjust the signal timer to 30 seconds on an NSF-capable router:

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

The following example shows how to adjust the signal timer to 30 seconds for EIGRP IPv6 NSF:

```
Device(config)# router eigrp e1
Device(config-router)# address-family ipv6 autonomous-system 1
Device(config-router-af)# timers nsf signal 30
```

Related Commands

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

vrf (call home)

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

vrf *name*
no vrf *name*

Syntax Description

name	Name of a configured VRF instance.

Command Default

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

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6 on the Cisco ASR 1000 Series Routers.
12.2(33)SRE1	This command was integrated into Cisco IOS Release 12.2(33)SRE1 on the Cisco 7200 Series Routers.

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

vrrp sso

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

vrrp sso
no vrrp sso

Syntax Description

This command has no arguments or keywords.

Command Default

VRRP support of SSO is enabled by default.

Command Modes

Global configuration (config)

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.