



Command Reference

This chapter describes Cisco 12000 Series Internet Router commands that are not described in the Cisco IOS Command Reference for Release 12.0S or in any Cisco IOS Feature Module document. It describes the following commands:

- [arp \(global\), page 4-2](#)
- [clear psar, page 4-4](#)
- [description, page 4-5](#)
- [diag, page 4-6](#)
- [exception linecard crashinfo, page 4-13](#)
- [exception warmstart, page 4-14](#)
- [export map, page 4-16](#)
- [hw-module reload, page 4-17](#)
- [hw-module warm-reboot \(Privileged EXEC\), page 4-18](#)
- [hw-module warm-reboot \(Global Configuration\), page 4-19](#)
- [ip pim sparse-mode-register, page 4-20](#)
- [ip route-cache flow, page 4-21](#)
- [ip verify unicast source reachable-via, page 4-24](#)
- [microcode \(Cisco IOS image\), page 4-26](#)
- [show frame-relay pvc, page 4-28](#)
- [show ip bgp dampening, page 4-30](#)
- [show led, page 4-33](#)

Final Review Draft November 30, 2007 - Cisco Confidential

arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** global configuration command. To remove an entry from the ARP cache, use the **no** form of this command.

```
arp [vrf vrf-name] ip-address hardware-address type [{alias | interface}]
```

```
no arp [vrf vrf-name] ip-address
```

Syntax Description

vrf	Configures static ARP entries for an individual Virtual Private Network (VPN) routing and forwarding table (VRF).
<i>vrf-name</i>	VPN routing and forwarding table name.
<i>ip-address</i>	IP address of the ARP entry.
<i>hardware-address</i>	48-bit hardware address of the ARP entry, in the format H.H.H.
<i>type</i>	Encapsulation description. For Ethernet interfaces, this is typically the arpa keyword. For Fiber Distributed Data Interface (FDDI) and Token Ring interfaces, this is always snap . Other possibilities are sap (HP's ARP type), smds , and srp-a or srp-b .
alias	(Optional) Indicates that the Cisco IOS software should respond to ARP requests as if it were the owner of the specified address.
<i>interface</i>	(Optional) Interface identifier.

Defaults

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was changed to include configuring static ARP entries per VRF.

Usage Guidelines

The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally do not need to specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
Router# arp 192.168.7.19 0800.0900.1834 arpa
```

Final Review Draft November 30, 2007 - Cisco Confidential

The following is an example of an ARP for a VRF:

```
Router(config)# arp vrf v4 20.1.1.1 0000.0000.0001 arpa
```

Related Commands	Command	Description
	clear arp-cache	Deletes all dynamic entries from the ARP cache.

Final Review Draft November 30, 2007 - Cisco Confidential

clear psar

To reset and restart all packet statistics maintained in the PRP segmentation and reassembly (PSAR) drivers, use the **clear psar** command in global configuration mode.

clear psar

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

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

Usage Guidelines The **clear psar** command replaces the **clear csar** command used on the Gigabit Route Processor.

Examples The following example shows how to clear all statistics recorded in the PSAR drivers:

```
Router# clear psar
```

Final Review Draft November 30, 2007 - Cisco Confidential

description

To enter comments about your Virtual Private Network (VPN) routing and forwarding (VRF) configuration, use the **description** VRF submode command.

description *text*

Syntax Description

<i>text</i>	Up to 80 characters of text describing this VRF.
-------------	--

Defaults

No default behavior or values.

Command Modes

VRF submode

Command History

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

Usage Guidelines

Use this command to provide descriptive text about a particular VRF.

Examples

The following is an example of the VRF **description** command:

```
Router(config-vrf)# description This is my 4th VRF
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
show ip vrf	Displays information about a VRF or all VRFs.

Final Review Draft November 30, 2007 - Cisco Confidential**diag**

To perform field diagnostics on a line card, Route Processor card (RP), including both the Performance Route Processor (PRP) and Gigabit Route Processor (GRP), Switch Fabric Card (SFC), or Clock Scheduler Card (CSC) in Cisco 12000 Series Internet Routers, use the **diag** command in privileged EXEC configuration mode. To halt a running field diagnostic session on a line card or RP, use the **diag halt** form of this command.

Cisco 12000 Series Internet Router line cards

diag *slot-number* [**mbus**] [**verbose**] [**wait**] [**full**] [**coe**] **source** {**tftp** | **flash**} *source_path*

diag *slot-number* **previous**

diag *slot-number* **halt**

Cisco 12000 Series Internet Router RPs

diag *slot-number* [**verbose**] [**wait**] [**full**] [**coe**]

diag *slot-number* **previous**

diag *slot-number* **halt**

Cisco 12008, Cisco 12012, and Cisco 12016 SFCs and CSCs

diag *slot-number* [**verbose**]

Syntax Description

slot-number	Slot number of the card you want to test.
source	Specifies the source path of the line card diagnostic image. The name of the image file is c12k-fdiagsbflc.120-22.2.S , where 120-22.2.S is the version number. For Flash cards, the source path would typically be slot0:c12k-fdiagsbflc.120-22.2.S or slot1:c12k-fdiagsbflc.120-22.2.S . The TFTP source path would typically be tftp://tftp_server_ip_address/my_directory/c12k-fdiagsbflc.120-22.2.S . This option is available and required for line card testing only. This keyword must be followed by either the tftp or flash keyword.
halt	(Optional) Stops the field diagnostic testing on the line card. This option is only available for line cards and RPs.
previous	(Optional) Displays previous test results (if any) for the card. This option is only available for line cards and RPs.
verbose	(Optional) Enables progress and error messages to be displayed on the console. By default, only the minimum status messages are displayed on the console, along with the final result. Due to the comprehensive nature of testing, testing without the verbose option will result in up to a 15-minute delay before any results are displayed. Cisco recommends that the verbose option be specified and results captured when communicating with Cisco TAC.

Final Review Draft November 30, 2007 - Cisco Confidential

wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the successful completion of the field diagnostic testing. If you use this keyword, you must use the microcode reload slot global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the RP recognizes the line card and downloads the Cisco IOS software image to the line card.
mbus	(Optional) Forces the download to use the MBus as the path to download the line card diagnostic image. Normally the switch fabric is used to move the image to the line card to be tested. This takes only a few seconds, but requires much of the line card to be functional. The MBus download can take more than 15 minutes to download, but requires very little of the line card to be functional. For testing the standby RP, only MBus download can be used, and this is the default mode. SFCs and CSCs are not tested with a downloaded image.
coe	(Optional) Continue On Error. Normally the field diagnostics stop immediately upon failing any one test within a test session. Using the coe keyword forces the testing to continue to the end of the internal test list, even if a failure occurs. Caution should be exercised because in some cases where a cascade of failures is found, using this option MAY require the router to be reloaded, affecting all RPs and line cards. This option is only available for line cards and RPs.
full	(Optional) The default set of tests emphasize memory and data path tests. To force the line card or RP to complete the most extensive set of tests, use the full option. The test time will be slightly longer. This option is only available for line cards and RPs.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 Series Internet Routers.
12.0(22)S	The source option was added for line cards.

Usage Guidelines

Before you can use the line card field diagnostics commands, you must place a valid diagnostics image on a separate Flash memory card installed in the Cisco 12000 Series Internet Router to be tested or on a TFTP boot server. The diagnostics image is named **c12k-fdiagsbflc-mz.120-22.S** (where 120-22.S is the version number) and is always available on Cisco.com.

RP, SFC, and CSC field diagnostics are embedded within the IOS image and thus do not require an external image.

The following Engine 0 line cards include components that are unable to isolate internal line card testing traffic from customer premise connections:

- 4-port OC-3/STM-1c POS
- 1-port OC-12/STM-4c POS

Final Review Draft November 30, 2007 - Cisco Confidential

- 4-port OC-3/STM-1c ATM
- 1-port OC-12c/STM-4c ATM

When testing these line cards, you are warned and notified to disconnect any connections to these line cards before testing to achieve the most reliable results and minimize traffic disruption.

The diagnostics software prompts you for confirmation before altering the router configuration. For example, running diagnostics on an SFC or CSC will cause the fabric to go from full bandwidth to one-quarter bandwidth. Bandwidth is not affected by RP or line card diagnostics.

Perform diagnostics on the CSC only if a redundant CSC is in the router. Diagnostics can be performed on redundant RPs only. Currently SFC and CSC testing is not available for Cisco 12400 Series Internet Routers.



Note

No cyclic redundancy check (CRC) error is reported in Cisco IOS software when a CRC error occurs on the Cisco 12010, 12410, or 12810 Internet Router. As a result, the faulty switch fabric card (SFC) is not shut down.

This problem has been resolved in IOS Release 12.0(26)S and later releases. However, in IOS Release 12.0(24)S or 12.0(25)S, if you suspect a switch fabric failure, you must use the **show controllers fia** command to display information about the Fabric Interface ASIC (FIA) controllers on the router. The FIA resides on both the Route Processor (RP) and line cards (LCs). It provides an interface between the RP/LC and the switch fabric cards.

As described in *Hardware Troubleshooting for the Cisco 12000 Series Internet Router*, enter the **show controllers fia** on the RP and on individual line cards to troubleshoot. Then take one of the following actions:

- If the results displayed by the **show controllers fia** command for line cards and the RP show CRC errors on the same SFC, verify that the card is correctly seated and then, if necessary, shut down and replace the SFC.
- If the results displayed by the **show controllers fia** command show that an SFC is faulty only on one line card, replace and then reload the line card.
- If the results displayed by the **show controllers fia** command show that more than one SFC is faulty on multiple line cards, replace primary clock and scheduler card (CSC).

For detailed information about the **show** command output, refer to *How To Read the Output of the Show Controller fia Command*.



Caution

Performing field diagnostics on a line card stops all activity on the line card. Before the **diag** command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

In normal mode, if a test fails, the title of the failed test is displayed on the console. However, not all tests that are performed are displayed. To view all performed tests, use the **verbose** keyword.

After all diagnostic tests are completed on the line card, a PASSED or TEST FAILURE message is displayed. If the line card sends a PASSED message, the Cisco IOS software image on the line card is automatically reloaded unless the **wait** keyword is specified. If the line card sends a TEST FAILURE message, the Cisco IOS software image on the line card is not automatically reloaded.

Final Review Draft November 30, 2007 - Cisco Confidential

If you want to reload the line card after it fails diagnostic testing, use the microcode **reload slot** global configuration command.

**Note**

When you stop the field diagnostic test using the **diag halt** command, the line card remains down (that is, in an unbooted state). Generally, you would stop testing in order to remove or replace the line card. If this is not the case, and you need to bring the line card back up (online), use the microcode **reload** global configuration command or power cycle the line card.

If the line card fails the test, the line card is defective and should be replaced. Under certain circumstances, TAC engineers may direct you to replace field-replaceable memory modules and retest. This should **ONLY** be done under the guidance of a TAC engineer. For example, if the DRAM test failed, a customer might only need to replace the DRAM on the line card.

For more information, refer to the appropriate Cisco 12000 Series Internet Router installation and configuration guide.

Examples

The following example shows the output when field diagnostics are performed on the line card in slot 7. After the line card passes all field diagnostic tests, the Cisco IOS software is automatically reloaded on the card. Before starting the diagnostic tests, you must confirm the request to perform these tests on the line card because all activity on the line card is halted. The message “total/indiv. timeout set to 2000/600 sec.” indicates that 2000 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 600 seconds to complete.

```
Router# diag 7 source tftp tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-22.S
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus' option.
Running Diags will halt ALL activity on the requested slot. [confirm]
award-rp-slot0#
Launching a Field Diagnostic for slot 7
Downloading diagnostic tests to slot 7 via fabric (timeout set to 300 sec.)
5d20h: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event: EV_ADMIN_FDIAG
Loading images/award/c12k-fdiagsbflc-mz.120-22.S from 192.164.1.1 (via Ethernet0):
!!!!
5d20h: Downloading diags from tftp file
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-22.S
!!!![OK - 13976524 bytes]
FD 7> *****
FD 7> GSR Field Diagnostics V6.05
FD 7> Compiled by award on Tue Jul 30 13:00:41 PDT 2002
FD 7> view: award-conn_isp.FieldDiagRelease
FD 7> *****
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 7> BFR_CARD_TYPE_OC12_4P_POS testing...
FD 7> Available test types 2
FD 7>
1
FD 7> Completed f_diags_board_discovery() (0x1)
FD 7> Test list selection received: Test ID 1, Device 0
FD 7> running in slot 7 (30 tests from test list ID 1)
FD 7> Skipping MBUS_FDIAG command from slot 2
FD 7> Just into idle state
Field Diagnostic ****PASSED**** for slot 7
Shutting down diags in slot 7
Board will reload
5d20h: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event: EV_ADMIN_FDIAG
SLOT 7:00:00:09: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
```

Final Review Draft November 30, 2007 - Cisco Confidential

```
IOS (tm) GS Software (GLC1-LC-M), Experimental Version 12.0(20020509:045149)
[award-conn_osp.f_diag_new 337]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 25-Jun-02 15:51 by award
```

The following example shows the output of a line card test with the **verbose** option specified (highly recommended).

```
Router# diag 7 verbose tftp tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-22.S
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus' option.
Verbose mode: Test progress and errors will be displayed
Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 7
Downloading diagnostic tests to slot 7 via fabric (timeout set to 300 sec.)
00:07:41: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event: EV_ADMIN_FDIAG
Loading images/award/c12k-fdiagsbflc-mz.120-22.S from 192.164.1.1 (via Ethernet0):
!!!!!! (...
00:08:24: Downloading diags from tftp file
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120.22.S
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13976524 bytes]
FD 7> *****
FD 7> GSR Field Diagnostics V6.05
FD 7> Compiled by award on Tue Jul 30 13:00:41 PDT 2002
FD 7> view: award-conn_osp.FieldDiagRelease
FD 7> *****
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 7> BFR_CARD_TYPE_OC12_4P_POS testing...
FD 7> Available test types 2
FD 7> 1
FD 7> Completed f_diags_board_discovery() (0x1)
FD 7> Verbosity now (0x00000011) TESTSDISP FATL
FD 7> Test list selection received: Test ID 1, Device 0
FD 7> running in slot 7 (30 tests from test list ID 1)
FD 7> Just into idle state
FDIAG_STAT_IN_PROGRESS(7): test #1 Dram Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #2 Dram Datapins
FDIAG_STAT_IN_PROGRESS(7): test #3 Dram Busfloat
FDIAG_STAT_IN_PROGRESS(7): test #4 RBM SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #5 RBM SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #6 RBM SSRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #7 RBM SSRAM Datapins Memory
FDIAG_STAT_IN_PROGRESS(7): test #8 TBM SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #9 TBM SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #10 TBM SSRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #11 TBM SSRAM Datapins Memory
FDIAG_STAT_IN_PROGRESS(7): test #12 PSA TLU SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #13 PSA TLU SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #14 PSA PLU SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #15 PSA PLU SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #16 PSA SRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #17 PSA SRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #18 To Fabric SOP FIFO SRAM Memory
FDIAG_STAT_IN_PROGRESS(7): test #19 From Fabric SOP FIFO SRAM Memory
FDIAG_STAT_IN_PROGRESS(7): test #20 RBM to SALSA Packet
FDIAG_STAT_IN_PROGRESS(7): test #21 TBM to SALSA Packet
FDIAG_STAT_IN_PROGRESS(7): test #22 RBM to TBM SLI Packet Loopback
FDIAG_STAT_IN_PROGRESS(7): test #23 TBM to PSA Packet - Frammer Loopback
FDIAG_STAT_IN_PROGRESS(7): test #24 TBM to TX SOP Packet
FDIAG_STAT_IN_PROGRESS(7): test #25 TBM to RX SOP Packet - 4302 Terminal Loopback
FDIAG_STAT_IN_PROGRESS(7): test #26 TBM to RX SOP Packet - Frammer System Bus Loop
```

Final Review Draft November 30, 2007 - Cisco Confidential

```

FDIAG_STAT_IN_PROGRESS(7): test #27 RBM to TBM Fabric Packet Loopback
FDIAG_STAT_IN_PROGRESS(7): test #28 TBM to RBM Packet, RBM page crossing
FDIAG_STAT_IN_PROGRESS(7): test #29 TBM to TX SOP Packet Simultaneous
FDIAG_STAT_IN_PROGRESS(7): test #30 TBM to PSA Multicast Packets - Framer Loopbac
FDIAG_STAT_DONE(7)
FD 7> Changed current_status to FDIAG_STAT_IDLE
Field Diagnostic ****PASSED**** for slot 7
Field Diag eeprom values: run 62 fail mode 0 (PASS) slot 7
last test failed was 0, error code 0
Shutting down diags in slot 7
Board will reload

```

Following is an example of a test FAILURE condition on a GRP card. This card would need to be replaced and returned to Cisco for repair:

```

Field Diag download COMPLETE for slot 3
FD 3> *****
FD 3> GSR Field Diagnostics V6.01
FD 3> Compiled by award on Tue Apr 9 07:22:53 PDT 2002
FD 3> view: award-conn_osp.f_diag_new
FD 3> *****
Diagnostics have been downloaded to slot 3
Executing all diagnostic tests in slot 3
(total/indiv. timeout set to 2000/600 sec.)
FD 3> BFRP w/ECC testing...
FD 3> Secondary Discovery found ID 2
FD 3> BFR_CARD_TYPE_BFRP_CARD w/ ECC testing...
FD 3> Available test types 2
FD 3> 1
FD 3> Completed f_diags_board_discovery() (0x1)
FD 3> Verbosity now (0x00000011) TESTSDISP FATL
FD 3> Test list selection received: Test ID 1, Device 0
FD 3> running in slot 3 (24 tests from test list ID 1)
FDIAG_STAT_IN_PROGRESS(3): test #1 BFRP Dram Datapins Test
FDIAG_STAT_IN_PROGRESS(3): test #2 Dram Marching Pattern Test
FDIAG_STAT_IN_PROGRESS(3): test #3 DataPins_Sram
FDIAG_STAT_IN_PROGRESS(3): test #4 March_Sram
FDIAG_STAT_IN_PROGRESS(3): test #5 High Memory DRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(3): test #6 diags_csar_regtest
FDIAG_STAT_IN_PROGRESS(3): test #7 diags_test_p4_csar_int
FDIAG_STAT_IN_PROGRESS(3): test #8 NVRAM Memory Test
FD 3> 32 bit data compare error. Wrote 0xcccccccc, read back 0xcc41cccc at location
0xbe03fff0
FDIAG_STAT_DONE_FAIL(3) test_num 8, error_code 1
COMPLETED Field Diags: pid 128, status 5, test_num 8, error_code 1
Field Diagnostic: ****TEST FAILURE**** slot 3: first test failed: 8,
NVRAM Memory Test, error 1
Field Diag results from eeprom before updating slot 3, run# 0x5000042 were 0x0
previous field diag eeprom values: run 66 fail mode 5 (DOWNLOAD FAILURE)
last test failed was 0, error code 0
Field Diag eeprom values: run 67 fail mode 1 (TEST FAILURE) slot 3
last test failed was 8, error code 1
Shutting down diags in slot 3
slot 3 done, will not reload automatically

```

The following example shows the previous test results of a line card. Diagnostics had been run 64 times on this line card. Because the board PASSED the last field diagnostics session, the fail mode was 0, as was the last test that failed.

```

Router # diag 7 prev
Field Diag eeprom values: run 64 fail mode 0 (PASS) slot 7
last test failed was 0, error code 0

```

Final Review Draft November 30, 2007 - Cisco Confidential**Related Commands**

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card on the Cisco 12000 Series Internet Routers after all microcode configuration commands have been entered.

Final Review Draft November 30, 2007 - Cisco Confidential

exception linecard crashinfo

To configure a Cisco 12000 Series Internet Router to save system crash information files in a location other than in the RP bootflash memory, use the **exception linecard crashinfo** command in global configuration mode. To specify that crash information data not be saved, use the **no** form of this command.

```
exception linecard {slot slot-number | all} crashinfo file file-name
```

```
no exception linecard {slot slot-number | all} crashinfo
```

Syntax Description

slot <i>slot-number</i>	Slot number of the line card for which you want configure the crashinfo file.
all	Configure the crashinfo file for all line cards in the chassis.

Defaults

By default the crashinfo file is saved to the RP bootflash.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.

Usage Guidelines

Line cards can generate a full crashinfo file that can be saved in nonvolatile storage. This is in addition to the mini-crashinfo that is saved in the RP RAM and can be viewed using the **show context** command.

By default, the line card crashinfo file is saved to the RP bootflash, with the name `crashinfo_yyyymmdd-hhmmss.x` where `x` is the slot number. For example, a crashinfo file from a line card in slot 3 would appear as follows:

```
16  -rw-      175232   Jan 15 2003 20:00:25 crashinfo_20030115-200025.3
```

Line card crashinfo files are only saved to the bootflash if there is a reasonable amount of spare space in the bootflash. The design intent is to reserve sufficient space for RP crashinfo files, even if there are multiple linecard failures.

The **no** form of the command disables the saving of the line card crashinfo data.

Use the **exception linecard crashinfo** command to specify a filename when the line card crashinfo data is to be saved in an alternative location.

Final Review Draft November 30, 2007 - Cisco Confidential

exception warmstart

To configure a Cisco 12000 Series Internet Router for a warmstart in case of a system crash, use the **exception warmstart** command in global configuration mode. To remove the warmstart configuration settings, use the **no** form of this command.

exception warmstart *min-uptime max-restarts* [**d**]

no exception warmstart *min-uptime max-restarts*

Syntax Description

<i>min-uptime</i>	Minimum amount of PRP uptime (in seconds) required before a warmstart is performed. Valid values are from 0 to 1000000.
<i>max-restarts</i>	Maximum number of IOS warmstarts allowed before a warmstart is no longer performed. Valid values are from 0 to 1000000.
d	Optional. Enables a warmstart if a second (dual) Performance Router Processor (PRP) is installed.

Defaults

The default for the minimum uptime is 60 seconds.

The default for the maximum number of restarts allowed is 5.

The warmstart feature defaults are as follows:

- Enabled if only one PRP is installed.
- Disabled if a second, standby PRP is installed in the router.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The warmstart feature allows the PRP in a Cisco 12000 Series Internet Router to restart the IOS software configuration after a crash, without having to reload the image from an external device.

**Note**

As with other **exception** commands, use the **exception warmstart** command only as instructed and when asked to do so by Cisco technical support personnel.

If the PRP has been running for at least the amount of time specified by *min-uptime*, and if the system has not been restarted more than the number of times specified by *max-restarts*, the route processor restarts the Cisco IOS following a system crash.

In a dual PRP configuration (that is, when a redundant PRP is installed in the router), the warmstart feature is disabled by default. For this reason, you must specify **d** (for **d**ual) when you enter the **exception warmstart** command to enable a warmstart.

Final Review Draft November 30, 2007 - Cisco Confidential

This feature does not affect the behavior of the **reload** command. Also, you can still perform a “send break” as usual from the console by pressing **Ctrl-Z**.

Examples

The following example applies to a redundant configuration in which two PRPs are installed. It shows how to configure a warmstart if the IOS software in the PRP has been running for at least 90 seconds, and if the system has not been restarted more than eight times:

```
Router# configure terminal  
Router# exception warmstart 90 8 d
```

Final Review Draft November 30, 2007 - Cisco Confidential

export map

To configure an export route map for a VRF, use the **export map** VRF submode command.

```
export map route-map
```

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an export route map for the VRF.
---------------------------	------------------	--

Defaults	There is no default. A VRF has no export route map unless one is configured using the export map command.	
-----------------	--	--

Command Modes	VRF submode	
----------------------	-------------	--

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

Usage Guidelines	Use an export route map when an application requires finer control over the routes in a VRF than provided by the import and export extended communities configured for importing and exporting VRF.
-------------------------	---

Examples	The following example shows how to configure an export route map for a VRF:
-----------------	---

```
Router(config)# ip vrf vrf_blue
Router(config-vrf)# export map blue_export_map
```

Related Commands	Command	Description
	ip vrf	Enters VRF configuration mode.
	route-target	Configures import and export extended community attributes for the VRF.
	show ip vrf	Displays information about a VRF or all VRFs.

Final Review Draft November 30, 2007 - Cisco Confidential

hw-module reload

To reload a line card, use the **hw-module reload** privileged EXEC command.

hw-module slot *slot-number* reload

Syntax Description	slot <i>slot-number</i> Slot number of the line card that you want to reload.				
Defaults	There are no defaults.				
Command Modes	Privileged EXEC				
Usage Guidelines	This command causes the line card to reset and redownload the Maintenance Bus (MBus) and Fabric Downloader software modules before attempting to redownload the line card Cisco IOS software.				
Examples	In the following example, the line card in slot 3 is reloaded. Router# hw-module slot 3 reload				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>microcode reload</td> <td>Reloads the Cisco IOS image on a line card.</td> </tr> </tbody> </table>	Command	Description	microcode reload	Reloads the Cisco IOS image on a line card.
Command	Description				
microcode reload	Reloads the Cisco IOS image on a line card.				

Final Review Draft November 30, 2007 - Cisco Confidential

hw-module warm-reboot (Privileged EXEC)

To initiate a warm reboot of a line card, use the **hw-module warm-reboot** privileged EXEC command.

```
hw-module slot slot-number warm-reboot
```

Syntax Description

slot *slot-number* Slot number of the line card that you want to reload.

Defaults

There are no defaults.

Command Modes

Privileged EXEC

Usage Guidelines

A warm reboot restarts the Cisco IOS image that is already installed on the line card. The effect is similar to a reload, except that the line card returns to service in a shorter amount of time.

If the line card is in a state where a warm reboot is not possible, then a full reload is performed.

A warm reboot does not reset any of the line card hardware.

Some line cards do not support a warm reboot. If you use this command on such a card, a reload is performed.

Examples

In the following example, the line card in slot 3 is warm rebooted.

```
Router# hw-module slot 3 warm-reboot
```

Related Commands

Command	Description
hw-module reload	Reloads the Cisco IOS image on a line card.

Final Review Draft November 30, 2007 - Cisco Confidential

hw-module warm-reboot (Global Configuration)

To enable warm reboots of a line card, use the **hw-module warm-reboot** global configuration command. To disable warm reboots on a line card, use the **no** form of this command.

hw-module slot *slot-number* warm-reboot

no hw-module slot *slot-number* warm-reboot

Syntax Description

slot *slot-number* Slot number of the line card that you want to reload.

Defaults

This command is enabled by default.

Command Modes

Global configuration

Usage Guidelines

This command enables or disables the use of warm reboot by the system to recover from possible line card problems. By default, warm reboot is enabled. If warm reboot is disabled using the **no** form of this command, line card failures will result in a full reload.

Having warm reboot enabled does not mean that the system will use this method of error recovery. The RP has a set of criteria for choosing the recovery method and will only use warm reboot in a limited set of instances.

If an automatic warm reboot fails, the system will perform a full reload of the card.

There may be specific line cards that do not support warm reboot. For these line cards, the warm reboot option is automatically disabled.

Examples

In the following example, the warm reboot on the line card in slot 3 is disabled.

```
Router(config)# no hw-module slot 3 warm-reboot
```

Related Commands

Command	Description
hw-module warm-reboot (Privileged EXEC)	Reloads the Cisco IOS image on a line card.

Final Review Draft November 30, 2007 - Cisco Confidential

ip pim sparse-mode-register

To register directly connected sources, use the **ip pim sparse-mode-register** command in interface configuration mode. Use the **no** form of this command to stop registering directly connected sources.

ip pim sparse-mode-register

no pim sparse-mode-register

Syntax Description This command has no arguments or keywords.

Defaults This command is enabled by default when PIM sparse-mode is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(18)S	This command was introduced.

Usage Guidelines The **ip pim sparse-mode-register** command is available on Cisco 12000 Series Internet Routers Packet-over-SONET (POS) interfaces on Engine 4 line cards, and the command only applies when PIM sparse-mode (for multicast) is enabled. By default, this command is enabled and stored in NVRAM as the default, and the router will perform normally. If **no ip pim sparse-mode-register** is configured, the router will not register directly connected sources. This action only affects sparse-mode groups, not dense-mode groups or source-specific-mode groups.

It is recommended that you configure **no ip pim sparse-mode-register** to save memory in hardware-forwarding database of Engine 4 line cards if you do not have directly connected sources, such as typical backbone links.

Final Review Draft November 30, 2007 - Cisco Confidential

ip route-cache flow

To enable NetFlow switching for IP routing, use the **ip route-cache flow** command in interface configuration mode. To disable NetFlow switching, use the **no** form of this command.

ip route-cache flow [**sampled** [**input** | **output**]]

no ip route-cache flow [**sampled** [**input** | **output**]]

Syntax Description

sampled	(Optional) Enables NetFlow cache in sampled mode.
input	(Default) Enables NetFlow sampling on inbound IP flows.
output	Enables NetFlow sampling on outbound flows

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(11)S	The sampled keyword was added.
12.0(22)S	The input and output keywords were added.

Usage Guidelines

NetFlow is an accounting and acceleration mechanism that captures a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type-of-service information that can be used for a wide variety of purposes, such as network analysis and planning, accounting, and billing. To export NetFlow data, use the **ip flow-export global** configuration command.

NetFlow is supported on IP and IP encapsulated traffic over all interface types and encapsulations except for Inter-Switch Link/VLAN, ATM, and Frame Relay interfaces when more than one input access control list is used on the interface, and ATM local area network emulation (LANE).

In conventional switching at the network layer, each incoming packet is handled on an individual basis with a series of functions to perform access list checks, capture accounting data, and switch the packet. With NetFlow, after a flow has been identified and access list processing of the first packet in the flow has been performed, all subsequent packets are handled on a “connection-oriented” basis as part of the flow, where access list checks are bypassed and statistics captures are performed in tandem.

A network flow is identified as a unidirectional stream of packets between a source and destination—both defined by a network-layer IP address and transport-layer port number. Specifically, a flow is identified as the combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number

Final Review Draft November 30, 2007 - Cisco Confidential

- Protocol type
- Type of service
- Input interface

NetFlow operates by creating a flow cache that contains the information needed to perform access list check for all active flows. The NetFlow cache is built by processing the first packet of a flow through the standard fast switching path. As a result, each flow is associated with an incoming and outgoing interface port number and with a specific security access permission and encryption policy. The cache also includes entries for traffic statistics that are updated in tandem with the switching of subsequent packets. After the NetFlow cache is created, packets identified as belonging to an existing flow have their traffic statistic counters incremented and security access list checks bypassed. Flow information is maintained within the NetFlow cache for all active flows.

NetFlow is not one of the available switching modes. When you configure NetFlow on an interface, you must have some other switching method to actually switch the packet. Also, with NetFlow you can export data (traffic statistics) to a remote workstation for further processing.

NetFlow accounting is based on identifying packet flows and maintaining statistics and access list processing within a router. It does not involve any connection-setup protocol—either between routers or to any other networking device or end station—and does not require any change externally—either to the traffic or packets themselves or to any other networking device. Thus, NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Because NetFlow is performed independently on each internetworking device, it does not need to be operational on each router in the network. Network planners can selectively invoke NetFlow accounting (and NetFlow data export) on a router/interface basis to gain traffic performance, control, or accounting benefits in specific network locations.

**Note**

When sampled NetFlow is disabled on an interface, normal NetFlow also becomes disabled. This restriction was made to prevent the interface from being overwhelmed by the sudden transition from sampled NetFlow to normal NetFlow. You need to explicitly reenable NetFlow if so desired. The default value for the sampling interval is four billion. This default packet interval was designed to protect the router from being choked by a misconfiguration. You need to explicitly configure a usable packet interval for your case.

**Note**

NetFlow consumes additional memory and CPU resources in comparison with other switching modes; therefore, it is important to understand the resources required on your router before enabling NetFlow.

**Note**

Full NetFlow does not work on Engine 2 line cards. Although you can complete the full configuration, only Sampled NetFlow will work.

Examples

The following example enables NetFlow switching on the interface:

```
interface ethernet 0/5/0
 ip address 17.252.245.2 255.255.255.0
 ip route-cache flow
```

Related Commands

Final Review Draft November 30, 2007 - Cisco Confidential

Command	Description
ip flow-export	Enables the exporting of information in NetFlow cache entries.

Final Review Draft November 30, 2007 - Cisco Confidential

ip verify unicast source reachable-via

To enable and configure Reverse Path Forwarding (RPF) checks, use the **ip verify unicast source reachable-via** command in interface configuration mode. Use the **no** form of this command to disable RPF.

```
ip veirfy unicast source reachable-via {any | rx} [allow-default] [allow-self-ping]
```

```
no ip veirfy unicast
```

Syntax Description

any	Checks that the source address is reachable on any path.
rx	Checks that the source address is reachable on the interface on which the packet was received.
allow-default	(Optional) Checks that the default route matches the source address.
allow-self-ping	(Optional) Allows the router to ping itself.

The optional *access-list*, **allow-self-ping**, **allow-default**, and **any** (enables loose checking mode) parameters, that are supported in the **ip verify unicast source reachable-via** command for IPv4 traffic on other platforms, are now supported for the **ipv6 verify unicast source reachable-via rx** command on the Cisco 12000 Series Internet Router with release 12.0(33)S.

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	Support for this command was introduced to the Cisco 12000 Series Internet Router IP services engine (ISE) line cards.

Usage Guidelines

Unicast RPF provides three basic modes:

- **Exists-only mode**—A source address need only be present in the Forwarding Information Base (FIB) and reachable through a “real” interface; this situation also applies to the **ip verify unicast source reachable-via any allow-default** command. The exists-only mode requires that a resolved and reachable source address is present in the FIB table. The source address must be reachable through a configured interface.
- **Any mode**—The source must be reachable through any of the paths. For example, the source has per-destination load balancing.
- **RX mode**—A source address must be reachable on the arrived interface. For example, the source must be reachable without load balancing.

Final Review Draft November 30, 2007 - Cisco Confidential

Note Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

To use Unicast RPF, enable Cisco Express Forwarding (CEF) switching or dCEF switching in the router. You do not need to configure the input interface for CEF switching. As long as CEF is running on the router, you can configure individual interfaces with other switching modes.



Note Unicast RPF will not work without CEF.

Do not use Unicast RPF on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, which means that there are multiple routes to the source of a packet. You should apply Unicast RPF only where there is natural or configured symmetry.

Examples

This example shows how to enable Unicast RPF exist-only checking mode:

```
Router(config-if)# ip verify unicast source reachable-via any
```

Related Commands

Command	Description
ip cef	Refer to Cisco IOS documentation

Final Review Draft November 30, 2007 - Cisco Confidential

microcode (Cisco IOS image)

To specify which Cisco IOS software image to load on a line card at reload, use the **microcode** global configuration command. To load the microcode bundled with the RP system image, use the **no** form of this command.

```
microcode {card-type card-type | slot slot-number} {flash file-id | tftp file-path}
```

```
no microcode {card-type card-type | slot slot-number} {flash file-id | tftp file-path}
```

Syntax Description

card-type <i>card-type</i>	Identifier of line card type that you want to copy the software image to. The identifier is a hexadecimal number between 0x21 and 0x79. Type a question mark (?) after the card-type keyword to see a list of valid card types.
slot <i>slot-number</i>	Slot number of the line card that you want to copy the software image to.
flash	Loads the image from the Flash file system.
<i>file-id</i>	Specifies the device and filename of the image file to download. A colon (:) must separate the device and filename (for example, slot0:gsr-p-mz). Valid devices are as follows: <ul style="list-style-type: none"> • bootflash—Internal Flash memory. • slot0—First PCMCIA slot. • slot1—Second PCMCIA slot.
tftp <i>file-path</i>	Loads the image from a TFTP server. <i>file-path</i> indicates the path to the TFTP server followed by the name of the image file.

Defaults

The image is loaded from the RP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2GS	This command was modified to load the Cisco IOS software image onto a line card in the Cisco 12000 Series Internet Routers.

Usage Guidelines

You must be in configuration mode to enter this command. The software image specified by this command is used when the system is booted, a line card is inserted or removed, or the microcode reload global configuration command is issued.

Immediately after you enter the **microcode reload** command and press **Return**, the system reloads all microcode. Global configuration mode remains enabled. After the reloading is complete, enter the exit command to return to the EXEC system prompt.

Final Review Draft November 30, 2007 - Cisco Confidential

In addition to the Cisco IOS image that resides on the RP, each line card on a Cisco 12000 Series Internet Router has a Cisco IOS image. When the router is reloaded, the specified Cisco IOS image is loaded onto the RP, and that image is automatically downloaded to all the line cards.

Normally, you want the same Cisco IOS image on the RP and all line cards. However, if you want to upgrade a line card with a new version of microcode for testing or to fix a defect, you might need to load a Cisco IOS image that is different from the one on the line card. Additionally, you might need to load a new image on the line card to work around a problem that is affecting only one of the line cards.

Examples

In the following example, the Cisco IOS software image in Flash disk slot 0: is downloaded to the line card in slot 10 and the line card is rebooted using this image.

```
Router(config)# microcode slot 10 flash slot0:fp.v141-7  
Router(config)# microcode reload 10  
Router(config)# exit
```

To verify that the correct version is loaded, use the **execute-on slot 10 show version** command.

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card.

Final Review Draft November 30, 2007 - Cisco Confidential

show frame-relay pvc

To display statistics about permanent virtual circuits (PVCs) for Frame Relay interfaces, use the **show frame-relay pvc** command in privileged EXEC mode.

```
show frame-relay pvc [interface interface] [dcli 64-bit]
```

Syntax Description	Parameter	Description
	interface	(Optional) Indicates a specific interface for which PVC information will be displayed.
	<i>interface</i>	(Optional) Interface number containing the DLCIs for which you wish to display PVC information.
	<i>dcli</i>	(Optional) A specific DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified.
	64-bit	Displays the 64-bit counters for the DLCI.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(1)T	This command was modified to display statistics about virtual access interfaces used for PPP connections over Frame Relay.
	12.0(3)XG	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
	12.0(4)T	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
	12.0(5)T	This command was modified to include information on the special voice queue that is created using the queue keyword of the frame-relay voice bandwidth command.
	12.1(2)T	This command was modified to include information about the policy map attached to a specified PVC.
	12.0(17)S	This command was modified to include the 64-bit keyword and include information about 64-bit counters.

Usage Guidelines Use this command to monitor the PPP link control protocol (LCP) state as being open with an “up” state, or closed with a “down” state.

When “voifr” or “voifr cisco” has been configured on the PVC, and a voice bandwidth has been allocated to the class associated with this PVC, configured voice bandwidth and used voice bandwidth are also displayed.

Final Review Draft November 30, 2007 - Cisco Confidential**Statistics Reporting**

To obtain statistics about PVCs on all Frame Relay interfaces, use this command with no arguments.

To obtain statistics about a PVC that include policy-map configuration, use this command with the DLCI argument.

Per-VC counters are not incremented at all when either autonomous or silicon switching engine (SSE) switching is configured; therefore, PVC values will be inaccurate if either switching method is used.

Traffic Shaping

Congestion control mechanisms are currently not supported, but the switch passes forward explicit congestion notification (FECN) bits, backward explicit congestion notification (BECN) bits, and discard eligible (DE) bits unchanged from entry to exit points in the network.

If a Local Management Interface (LMI) status report indicates that a PVC is not active, it is marked as inactive. A PVC is marked as deleted if it is not listed in a periodic LMI status message.

Examples

For detailed examples and explanations of displayed fields, refer to <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtfrpqfq.htm#xtocid26>

Related Commands

Command	Description
frame-relay pvc	Configures Frame Relay PVCs for FRF.8 Frame Relay-ATM Service Interworking.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.
show interfaces serial	Displays information about a serial interface.
show policy-map interface	Displays the configuration of classes configured for service policies on the specified interface or PVC.
show traffic-shape queue	Displays information about the elements queued at a particular time at the VC (DLCI) level.

Final Review Draft November 30, 2007 - Cisco Confidential

show ip bgp dampening

To display BGP dampened routes, use the **show ip bgp dampening EXEC** command.

show ip bgp dampening dampened-paths

show ip bgp dampening flap-statistics [**regex** *regex* | **quote-exp** *quoteexp* | **filter-list** *access-list* | **cidr-only** | **ip-address** *mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*len*]]]

show ip bgp dampening parameters

Syntax Description		
dampened-paths		Displays BGP dampened routes.
flap-statistics		Displays BGP flap statistics.
regex <i>regex</i>		(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-exp <i>quoteexp</i>		(Optional) Displays flap statistics for all the paths that match the regular expression contained within double quotes.
filter-list <i>access-list</i>		(Optional) Displays flap statistics for all the paths that pass the access list.
cidr-only		Displays flap statistics only for paths with non-natural netmasks.
<i>ip-address</i>		(Optional) Displays flap statistics for a single entry at this IP address.
<i>mask</i>		(Optional) Network mask applied to the value.
longer-prefixes		(Optional) Displays route and more specific routes.
injected		(Optional) Displays more specifics injected due to this prefix.
shorter-prefixes		(Optional) Displays less specific routes.
<i>len</i>		(Optional) Display prefixes longer than this mask length.
parameters		Displays details of the configured dampening parameters.

Defaults

There are no defaults.

Command Modes

EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.

Usage Guidelines

This command replaces the two commands **show ip bgp dampened-paths** and **show ip bgp flap-statistics**. It also adds the functionality of the **parameters** keyword.

Final Review Draft November 30, 2007 - Cisco Confidential**Examples**

The following is sample output from the **show ip bgp dampened-paths** command in privileged EXEC mode:

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From           Reuse    Path
*d 10.0.0.0         171.69.232.177 00:18:4 100 ?
*d 12.0.0.0         171.69.232.177 00:28:5 100 ?
```

Table 4-1 describes the significant fields shown in the display.

Table 4-1 show ip bgp dampening dampened-paths

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

The following is sample output from the **show ip bgp flap-statistics** command in privileged EXEC mode:

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From           Flaps Duration Reuse    Path
*d 10.0.0.0         171.69.232.177 4      00:13:31 00:18:10 100
*d 12.0.0.0         171.69.232.177 4      00:02:45 00:28:20 100
```

Table 4-2 describes the significant fields shown in the display.

Table 4-2 show ip bgp dampening flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.

Final Review Draft November 30, 2007 - Cisco Confidential**Table 4-2** show ip bgp dampening flap-statistics Field Descriptions (continued)

Field	Description
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

The following is sample output for the **show ip bgp dampening parameters** command:

```
Router# show ip bgp dampening parameters
dampening 10 1590 3000 30
Half-life time : 10 mins Decay Time : 1250 secs
Max suppress penalty: 12720 Max suppress time: 30 mins
Suppress penalty : 3000 Reuse penalty : 1590
```

Table 4-3 describes the significant fields.

Table 4-3 show ip bgp dampening parameters Field Descriptions

Field	Description
Half-life time	Configured value of half-life time (in minutes).
Decay time	Time (in seconds) for the penalty value to decay from maximum suppress penalty to suppress penalty. Note This value should not be too low.
Suppress penalty	Configured value of suppress penalty. A route is suppressed when its penalty exceeds this limit. The range is 1 to 20000; the default is 2000.
Reuse penalty	Configured value of reuse penalty. If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is 1 to 20000; the default is 750.
Max suppress time	Configured value of maximum suppress time (the maximum time, in minutes, that a route can be suppressed). The range is 1 to 20000; the default is 4 times the half-life. If the half-life value is allowed to default, the maximum suppress time defaults to 60 minutes.
Max suppress penalty	Calculated based on reuse penalty and maximum suppress time. When a route is penalized, its penalty value increases. The penalty cannot increase more than the maximum suppress penalty.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route-dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.
clear ip bgp dampening	Clears BGP route-dampening information and unsuppresses the suppressed routes.

Final Review Draft November 30, 2007 - Cisco Confidential

show led

To display the current status of all line card Light Emitting Diodes (LEDs), use the **show led** EXEC command.

```
show led [slot-number]
```

Syntax Description	slot-number	Slot number of the line card that you want display the LEDs for.
Defaults	There are no defaults.	
Command Modes	User EXEC	
Command History	Release	Modification
	11.2(09)GS	This command was introduced.

Usage Guidelines This command displays the status of the line card LEDs and is useful if you are performing remote configuration or troubleshooting of a router.

Examples In the following example, the LED status of all line cards is displayed:

```
Router# show led
SLOT 1 : RUN IOS
SLOT 6 : DNLD FABL
SLOT 7 : RP ACTV
SLOT 10 : RUN IOS
SLOT 11 : RUN IOS
SLOT 13 : RUN IOS
SLOT 14 : RUN IOS
```

The most common types of output that you see from this command and their meanings are described in the tables below.



Note If you have changed the displayed LED message using the **set card-message** command, it will be different than that specified here. These are default values only.



Note It is possible for the value of the LED to be reversed. For example, IOS RUN may be displayed as RUN IOS.

Final Review Draft November 30, 2007 - Cisco Confidential

Route Processor (RP) LED Status	Description
RP UP	RP is running Cisco IOS software and functioning correctly.
MSTR RP	RP is acting as the primary RP.
SLAV RP	RP is acting as the slave RP.
RP ACTV	RP is acting as the primary RP.
RP SEC	RP is acting as the slave RP.
MEM INIT	RP is trying to size the memory.

Line Card LED Status	Description
DIAG DNLD	Line card is downloading field diagnostic software.
DIAG FAIL	Line card has failed field diagnostic test.
DIAG PASS	Line card has passed field diagnostic test.
DIAG TEST	Line card is executing field diagnostic software.
FABL DNLD	Line card is launching Fabric Downloader.
FABL WAIT	Line card is waiting to load Fabric Downloader.
IN RSET	Line card is resetting.
IOS DNLD	Line card is downloading Cisco IOS software through the switch fabric.
IOS RUN	Line card is not enabled.
IOS UP	Line card has finished loading and is now running Cisco IOS software.
MBUS DNLD	Line card is downloading Maintenance Bus (Mbus) agent.
MEM INIT	Line card is trying to size memory.
PWR OFF	Line card is powered off.

If the line card status is anything other than “IOS RUN”, or the RP is neither the active Master/Primary nor the Slave/Secondary, there is a problem and the card has not fully loaded correctly.

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card.
set card-message	Specifies the message that is displayed on the LED on the front panel of one or more line cards.