## CONTENTS

**Full Cisco Trademarks with Software License**

### CHAPTER 1

**Introduction**

- Introduction 2
  - Cisco IOS IFS Command Syntax 2
  - Obtaining Documentation Obtaining Support and Security Guidelines 4

### CHAPTER 2

**A through B**

- activation-character 6
- alias 6
- archive 10
- archive config 11
- archive log config persistent save 13
- archive tar 14
- async-bootp 16
- attach 18
- autobaud 21
- auto-sync 22
- autoupgrade disk-cleanup 24
- autoupgrade ida url 25
- autoupgrade status email 26
- banner exec 27
- banner incoming 29
- banner login 31
- banner motd 32
configure check syntax  82
configuration mode exclusive  83
configure confirm  89
configure memory  90
configure network  91
configure overwrite-network  91
configure replace  91
configure revert  95
configure terminal  97
confreg  98
continue (ROM monitor)  100
copy  101
copy erase flash  120
copy http  120
copy https  120
copy logging system  120
copy xmodem  122
copy ymodem  123
copy noverify  124

CHAPTER 4  129
D through E  130
databits  130
data-character-bits  131
default-value data-character-bits  132
default-value exec-character-bits  132
default-value modem-interval  133
default-value special-character-bits  134
define interface-range  135
delete  136
diag  139
diagnostic bootup level  141
diagnostic cns  142
diagnostic event-log size  144
F through K 198
  file privilege 198
  file prompt 198
  file verify auto 199
  format 200
  fsck 204
  full-help 209
  help 211
  hidekeys 212
  history 213
  history size 215
  hold-character 216
  hostname 216
  hw-module reset 218
  hw-module shutdown 219
  insecure 219
  install 220
  international 223
  ip bootp server 224
  ip finger 225
  ip ftp passive 226
  ip ftp password 227
  ip ftp source-interface 228
  ip ftp username 229
  ip rarp-server 230
  ip rcmd domain-lookup 232
  ip rcmd rcp-enable 233
  ip rcmd remote-host 234
  ip rcmd remote-username 236
  ip rcmd rsh-enable 237
  ip rcmd source-interface 238
  ip telnet source-interface 240
  ip tftp blocksize 240
  ip tftp boot-interface 241
ip tftp min-timeout 242
ip tftp source-interface 242
ip wcep web-cache accelerated 244

CHAPTER 6  L through mode 247

L through mode 248
length 248
load-interval 248
location 250
lock 251
lockable 252
log config 253
logging buffered 254
logging buginf 257
logging enable 258
logging esm config 259
logging event bundle-status 260
logging event link-status (global configuration) 261
logging event link-status (interface configuration) 262
logging event subif-link-status 263
logging event trunk-status 264
logging reload 265
logging ip access-list cache (global configuration) 266
logging ip access-list cache (interface configuration) 268
logging persistent (config-archive-log-cfg) 269
logging persistent reload (config-archive-log-cfg) 270
logging size 271
logging synchronous 272
logging system 275
logout 276
logout-warning 277
macro (global configuration) 277
macro (interface configuration) 279
maximum 280
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory cache error-recovery</td>
<td>282</td>
</tr>
<tr>
<td>memory cache error-recovery options</td>
<td>283</td>
</tr>
<tr>
<td>memory free low-watermark</td>
<td>284</td>
</tr>
<tr>
<td>memory lite</td>
<td>285</td>
</tr>
<tr>
<td>memory reserve</td>
<td>285</td>
</tr>
<tr>
<td>memory reserve critical</td>
<td>287</td>
</tr>
<tr>
<td>memory sanity</td>
<td>288</td>
</tr>
<tr>
<td>memory scan</td>
<td>289</td>
</tr>
<tr>
<td>memory-size iomem</td>
<td>289</td>
</tr>
<tr>
<td>menu (EXEC)</td>
<td>290</td>
</tr>
<tr>
<td>menu menu-name single-space</td>
<td>292</td>
</tr>
<tr>
<td>menu clear-screen</td>
<td>293</td>
</tr>
<tr>
<td>menu command</td>
<td>294</td>
</tr>
<tr>
<td>menu default</td>
<td>296</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>297</td>
</tr>
<tr>
<td>menu options</td>
<td>298</td>
</tr>
<tr>
<td>menu prompt</td>
<td>299</td>
</tr>
<tr>
<td>menu status-line</td>
<td>300</td>
</tr>
<tr>
<td>menu text</td>
<td>301</td>
</tr>
<tr>
<td>menu title</td>
<td>302</td>
</tr>
<tr>
<td>microcode (12000)</td>
<td>304</td>
</tr>
<tr>
<td>microcode (7000/7500)</td>
<td>305</td>
</tr>
<tr>
<td>microcode (7200)</td>
<td>306</td>
</tr>
<tr>
<td>microcode reload (12000)</td>
<td>307</td>
</tr>
<tr>
<td>microcode reload (7000 7500)</td>
<td>308</td>
</tr>
<tr>
<td>microcode reload (7200)</td>
<td>309</td>
</tr>
<tr>
<td>mkdir</td>
<td>310</td>
</tr>
<tr>
<td>mkdir disk0:</td>
<td>311</td>
</tr>
<tr>
<td>mode</td>
<td>312</td>
</tr>
<tr>
<td>monitor event-trace through Q</td>
<td>317</td>
</tr>
<tr>
<td>monitor event-trace through Q</td>
<td>318</td>
</tr>
<tr>
<td>monitor event-trace (EXEC)</td>
<td>318</td>
</tr>
<tr>
<td>monitor event-trace (global)</td>
<td>321</td>
</tr>
</tbody>
</table>
ping ip 381
ping srb 384
ping vrf 385
platform shell 388
power enable 389
power redundancy-mode 390
printer 390
private 392
process cpu statistics limit entry-percentage 393
process cpu threshold type 394
process-max-time 395
prompt 396
prompt config 397
pwd 397

CHAPTER 8 R through setup 399
R through setup 400
refuse-message 400
regexp optimize 401
reload 401
remote command 405
remote login 406
remote-span 408
rename 408
request platform software package describe file 409
request platform software package expand file 415
request platform software package install commit 417
request platform software package install file 418
request platform software package install rollback 426
request platform software package install snapshot 427
request platform software process release 429
request platform software system shell 430
request platform software shell session output format 431
request platform software snapshot 433
request platform software vty attach 435
revision 436
rmdir 437
rommon-pref 438
route-converge-interval 439
rsh 440
scheduler allocate 441
scheduler heapcheck enable 442
scheduler heapcheck poll 443
scheduler heapcheck process 444
scheduler interrupt mask profile 445
scheduler interrupt mask size 446
scheduler interrupt mask time 447
scheduler interval 448
scheduler isr-watchdog 449
scheduler max-sched-time 449
scheduler process-watchdog 450
scheduler timercheck process 451
scheduler timercheck system context 452
send 452
service compress-config 454
service config 455
service counters max age 457
service decimal-tty 458
service exec-wait 458
service finger 459
service hide-telnet-address 459
service linenuumber 460
service nagle 461
service prompt config 462
service sequence-numbers 463
service slave-log 463
service tcp-keepalives-in 464
service tcp-keepalives-out 465
service tcp-small-servers 465
service telnet-zerooidle 467
service timestamps 467
service udp-small-servers 472
service-module apa traffic-management 473
service-module wlan-ap bootimage 474
service-module wlan-ap reload 475
service-module wlan-ap reset 477
service-module wlan-ap session 478
service-module wlan-ap statistics 479
service-module wlan-ap status 480
session slot 481
set memory debug incremental starting-time 482
setup 483

CHAPTER 9

show through show fm summary 491

show through show fm summary 492

show 492

show command append 493

show command begin 494

show command exclude 496

show command include 498

show command redirect 500

show command section 501

show command tee 502

show (Flash filesystem) 503

show aliases 512

show alignment 512

show archive 515

show archive config differences 517

show archive config incremental-diffs 519

show archive config rollback timer 521

show archive log config 522

show as5400 526
show async boot
show autoupgrade configuration unknown
show bcm560x
show bootflash:
show bootvar
show buffers
show c2600
show c7200
show catalyst6000
show cls
show config id
show configuration id
show configuration lock
show context
show controllers (GRP image)
show controllers (line card image)
show controllers logging
show controllers tech-support
show coverage history
show data-corruption
show debugging
show declassify
show derived-config
show diagnostic cns
show diagnostic sanity
show disk
show disk0:
show disk1:
show environment
show environment alarm
show environment connector
show environment cooling
show environment status
show environment temperature
show errdisable detect 629
show errdisable recovery 630
show fastblk 630
show file descriptors 632
show file information 633
show file systems 634
show flh-log 636
show fm inspect 636
show fm interface 637
show fm reflexive 640
show fm summary 640
show funi 641
show identity policy 644
show identity profile 645
show install 646
show platform software snapshot status 647

CHAPTER 10

show gsr through show monitor event trace 649

show gsr through show monitor event trace 650
  show gsr 650
  show gt64010 (7200) 651
  show hardware 652
  show health-monitor 653
  show history 654
  show history all 655
  show hosts 657
  show html 660
  show idb 661
  show idprom 662
  show inventory 668
  show location 671
  show logging 673
  show logging count 679
  show logging history 681
show ip ports all 683
show logging system 685
show logging xml 687
show memory 689
show memory allocating-process 695
show memory dead 697
show memory debug incremental 699
show memory debug leaks 701
show memory debug references 708
show memory debug unused 709
show memory detailed 710
show memory ecc 716
show memory events 718
show memory failures alloc 719
show memory fast 720
show memory fragment 722
show memory lite-chunks 725
show memory multibus 727
show memory pci 728
show memory processor 729
show memory scan 733
show memory statistics history 735
show memory traceback 737
show memory transient 738
show microcode 739
show mls statistics 740
show module 742
show monitor event-trace 745

CHAPTER 11 show monitor permit list through show process memory 751

show monitor permit list through show process memory 752
show monitor permit-list 752
show monitor session 752
show msfc 757
CHAPTER 12  show protocols through showmon  877

show protocols through showmon  878
show protocols 878
show region 882
show registry 884
show reload 887
show resource-pool queue 887
show rhosts 889
show rom-monitor 890
show rom-monitor slot 892
show running identity policy 893
show running identity profile 894
show running-config 895
show running-config control-plane 902
show running-config map-class 903
show running-config partition 905
show scp 908
show slot 910
show slot0: 913
show slot1: 916
show software authenticity file 918
show software authenticity keys 920
show software authenticity running 921
show software package 923
show software installer rollback-timer 927
show stacks 928
show startup-config 930
show subsys 930
show sup-bootflash 931
show system jumbomtu 934
show tech-support 934
show template 942
show usb controllers 943
show usb device 945
show usb driver 947
show usb port 949
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show usb tree</td>
<td>949</td>
</tr>
<tr>
<td>show usbtoken</td>
<td>950</td>
</tr>
<tr>
<td>show version</td>
<td>951</td>
</tr>
<tr>
<td>show warm-reboot</td>
<td>974</td>
</tr>
<tr>
<td>show wiretap</td>
<td>975</td>
</tr>
<tr>
<td>show whoami</td>
<td>976</td>
</tr>
<tr>
<td>showmon</td>
<td>977</td>
</tr>
</tbody>
</table>

**CHAPTER 13**

**slave auto-sync config through terminal-type**

- slave auto-sync config through terminal-type
- slave auto-sync config
- slave default-slot
- slave image
- slave reload
- slave sync config
- slave terminal
- software clean
- software commit
- software expand
- software install file
- software install source switch
- software provision
- software repackage
- software rollback
- software source list
- software uninstall
- special-character-bits
- squeeze
- stack-mib portname
- state-machine
- stopbits
- storm-control level
- sync-restart-delay
systat 1022
system flowcontrol bus 1023
system jumbomtu 1023
tdm clock priority 1024
terminal databits 1026
terminal data-character-bits 1027
terminal dispatch-character 1028
terminal dispatch-timeout 1029
terminal download 1029
terminal editing 1030
terminal escape-character 1031
terminal exec-character-bits 1032
terminal flowcontrol 1033
terminal full-help 1034
terminal history 1035
terminal history size 1036
terminal hold-character 1038
terminal international 1039
terminal keymap-type 1040
terminal length 1040
terminal monitor 1041
terminal notify 1042
terminal padding 1043
terminal parity 1043
terminal rxspeed 1044
terminal special-character-bits 1045
terminal speed 1046
terminal start-character 1047
terminal stopbits 1047
terminal stop-character 1048
terminal telnet break-on-ip 1049
terminal telnet refuse-negotiations 1050
terminal telnet speed 1050
terminal telnet sync-on-break 1051
terminal telnet transparent 1052
terminal terminal-type 1052
terminal txspeed 1053
terminal width 1054
terminal-queue entry-retry-interval 1055
terminal-type 1055

test cable-diagnostics through xmodem 1057
test cable-diagnostics through xmodem 1058
test cable-diagnostics 1058
test flash 1059
test interfaces 1060
test memory 1061
test memory destroy 1061
test platform police get 1062
test platform police set 1063
tftp-server 1064
tftp-server system 1067
time-period 1067
trace (privileged) 1068
trace (user) 1072
traceroute 1074
traceroute mac 1077
undelete 1080
unprofile 1082
upgrade automatic abortversion 1082
upgrade automatic getversion 1083
upgrade automatic runversion 1086
upgrade filesystem monlib 1087
upgrade rom-monitor 1088
upgrade filesystem monlib 1092
upgrade rom-monitor preference 1093
vacant-message 1094
verify 1095
vtp 1100
warm-reboot 1103
where 1104
width 1105
write core 1106
write erase 1107
write memory 1107
write mib-data 1108
write network 1109
write terminal 1110
xmodem 1110

CHAPTER 15

ASCII Character Set and Hexadecimal Values 1113

ASCII Character Set and Hexadecimal Values 1114
Introduction

- Introduction, on page 2
Introduction

The *Cisco IOS Configuration Fundamentals Command Reference* provides command documentation associated with the following tasks:

- Using the Cisco IOS Command-Line Interface (CLI)
- Configuration Using Setup and AutoInstall
- Configuring Operating Characteristics for Terminals
- Managing Connections, Logins, Menus, and System Banners
  - Configure user menus and banners
- Using the Cisco Web Browser User Interface (UI)
  - Using the HTTP server-based UI as an alternative to the CLI
- Using the Cisco IOS Integrated File System (IFS)
  - The basics of filesystem use and Cisco IOS software’s filesystem infrastructure
- Configuring Basic File Transfer Services
  - Copy, move, and delete files locally or across the network
- Managing Configuration Files
- Loading, Maintaining, and Upgrading System Images
- Rebooting

For further information about performing these tasks, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* for your release.

---

**Note**

Some commands previously documented in this *Command Reference* have been moved to other books:

- Commands related to system management and network monitoring can be found in the *Cisco IOS Network Management Command Reference*. Command reference documentation for the Cisco IOS software feature “Service Assurance Agent (SAA)” can be found in the *Cisco IOS IP SLAs Command Reference*.

---

**Cisco IOS IFS Command Syntax**

Some commands in this book use URLs (uniform resource locators) as part of the command syntax. URLs used in the Cisco IOS Integrated File System (IFS) contain two parts: a file system or network prefix, and a file identification suffix. The following tables list URL keywords that can be used in the `source-url` and `destination-url` arguments for all commands in this book. The prefixes listed below can also be used in the `filesystem` arguments in this document.

The following table lists common URL network prefixes used to indicate a device on the network.
Table 1: Network Prefixes for Cisco IFS URLs

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>Specifies a File Transfer Protocol (FTP) network server.</td>
</tr>
<tr>
<td>rcp</td>
<td>Specifies an remote copy protocol (rcp) network server.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP server.</td>
</tr>
</tbody>
</table>

The following table lists the available suffix options (file identification suffixes) for the URL prefixes used in the previous table.

Table 2: File ID Suffixes for Cisco IFS URLs

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Suffix Options</th>
</tr>
</thead>
</table>
| ftp    | [[//[username[:password]@]location]/directory]/filename  
 For example:  
 ftp://network-config (prefix ://filename)  
 ftp://user1:mypassword1@example.com/config-files |
| rcp    | rcp:[//[username@]location]/directory]/filename |
| tftp   | tftp:[//location]/directory]/filename |

The following table lists common URL prefixes used to indicate memory locations on the system.

Table 3: File System Prefixes for Cisco IFS URLs

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>Boot flash memory.</td>
</tr>
<tr>
<td>disk0:</td>
<td>Rotating disk media.</td>
</tr>
<tr>
<td>flash: partition-number</td>
<td>Flash memory. This prefix is available on all platforms. For platforms that do not have a device named flash:, the prefix flash: is aliased to slot0:. Therefore, you can use the prefix flash: to refer to the main Flash memory storage area on all platforms.</td>
</tr>
<tr>
<td>flh:</td>
<td>Flash load helper log files.</td>
</tr>
<tr>
<td>null:</td>
<td>Null destination for copies. You can copy a remote file to null to determine its size.</td>
</tr>
<tr>
<td>nvram:</td>
<td>NVRAM. This is the default location for the running-configuration file.</td>
</tr>
<tr>
<td>slavebootflash:</td>
<td>Internal Flash memory on a slave RSP card of a router configured with Dual RSPs.</td>
</tr>
<tr>
<td>slavevram:</td>
<td>NVRAM on a slave RSP card.</td>
</tr>
<tr>
<td>slaveslot0:</td>
<td>First PCMCIA card on a slave RSP card.</td>
</tr>
</tbody>
</table>
Prefix          Description

slaveslot1:     Second PCMCIA card on a slave RSP card.

slot0:          First PCMCIA Flash memory card.

slot1:          Second PCMCIA Flash memory card.

xmodem:         Obtain the file from a network machine using the Xmodem protocol.

ymodem:         Obtain the file from a network machine using the Ymodem protocol.

For details about the Cisco IOS IFS, and for IFS configuration tasks, refer to the “Using the Cisco IOS Integrated File System (IFS)” chapter in the latest Cisco IOS Configuration Fundamentals Configuration Guide appropriate for your release version.

Obtaining Documentation Obtaining Support and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

A through B

- A through B, on page 6
activation-character

To define the character you enter at a vacant terminal to begin a terminal session, use the `activation-character` command in line configuration mode. To make any character activate a terminal, use the `no` form of this command.

```
activation-character  ascii-number
no  activation-character
```

**Syntax Description**
- `ascii-number`: Decimal representation of the activation character.

**Command Default**
- Return (decimal 13)

**Command Modes**
- Line configuration (config-line)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>This command is supported in all Cisco IOS software Releases.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

See the “ASCII Character Set and Hexadecimal Values” document for a list of ASCII characters.

**Note**

If you are using the `autoselect` function, set the activation character to the default, Return, and exec-character-bits to 7. If you change these defaults, the application will not recognize the activation request.

**Examples**

The following example shows how to set the activation character for the console to Delete, which is decimal character 127:

```
Router(config)# line console
Router(config-line)# activation-character 127
```

alias

To create a command alias, use the `alias` command in global configuration mode. To delete all aliases in a command mode or to delete a specific alias, and to revert to the original command syntax, use the `no` form of this command.

```
alias  mode command-alias original-command
no alias  mode  [command-alias]
```
Syntax Description

<table>
<thead>
<tr>
<th>Command Alias</th>
<th>Original Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode</td>
<td>Command mode of the original and alias commands.</td>
</tr>
<tr>
<td>command-alias</td>
<td>Command alias.</td>
</tr>
<tr>
<td>original-command</td>
<td>Original command syntax.</td>
</tr>
</tbody>
</table>

Command Default

A set of six basic EXEC mode aliases are enabled by default. See the “Usage Guidelines” section of this command for a list of default aliases.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0M</td>
<td>The command <strong>alias ip-vrf</strong> has been replaced with <strong>alias vrf-af</strong>.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can use simple words or abbreviations as command aliases.

The table below lists the basic EXEC mode aliases that are enabled by default.

Table 4: Default Command Aliases

<table>
<thead>
<tr>
<th>Command Alias</th>
<th>Original Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>help</td>
</tr>
<tr>
<td>lo</td>
<td>logout</td>
</tr>
<tr>
<td>p</td>
<td>ping</td>
</tr>
<tr>
<td>r</td>
<td>resume</td>
</tr>
<tr>
<td>s</td>
<td>show</td>
</tr>
<tr>
<td>w</td>
<td>where</td>
</tr>
</tbody>
</table>

The default aliases in the table above are predefined. These default aliases can be disabled with the **no alias exec** command.

Common keyword aliases (which cannot be disabled) include **running-config** (keyword alias for **system:running-config**) and **startup-config** (keyword alias for **nvram:startup-config**). See the description of the **copy** command for more information about these keyword aliases.

Note that aliases can be configured for keywords instead of entire commands. You can create, for example, an alias for the first part of any command and still enter the additional keywords and arguments as normal.

To determine the value for the mode argument, enter the command mode in which you would issue the original command (and in which you will issue the alias) and enter the ? command. The name of the command mode should appear at the top of the list of commands. For example, the second line in the following sample output shows the name of the command mode as “Interface configuration”:
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface e0
Router(config-if)#?
Interface configuration commands:
   access-expression     Build a bridge boolean access expression
   .
   .

To match the name of the command mode to the acceptable mode keyword for the alias command, issue the alias ? command. As shown in the following sample output, the keyword needed to create a command alias for the access-expression command is interface:

Router(config)# alias interface express access-expression

When you use online help, command aliases are indicated by an asterisk (*), and displayed in the following format:
*command-alias =original-command

For example, the lo command alias is shown here along with other EXEC mode commands that start with “lo”:

Router# lo?
*lo=logout lock login logout

When you use online help, aliases that contain multiple keyword elements separated by spaces are displayed in quotes, as shown here:

Router(config)#alias exec device-mail telnet device.cisco.com 25
Router(config)#end
Router#device-mail?
*device-mail="telnet device.cisco.com 25"

To list only commands and omit aliases, begin your input line with a space. In the following example, the alias td is not shown, because there is a space before the t?command line.

Router(config)#alias exec td telnet device
To circumvent command aliases, use a space before entering the command. In the following example, the command alias *express* is not recognized because a space is used before the command.

```
Router(config-if)#exp?
*express-access-expression
Router(config-if)# express ?
```

As with commands, you can use online help to display the arguments and keywords that can follow a command alias. In the following example, the alias *td* is created to represent the command *telnet device*. The /debug and /lineswitches can be added to *telnet device* to modify the command:

```
Router(config)#alias exec td telnet device
```

You must enter the complete syntax for the command alias. Partial syntax for aliases is not accepted. In the following example, the parser does not recognize the command *t* as indicating the alias *td*:

```
Router# t
% Ambiguous command: "t"
```

**Examples**

In the following example, the alias *fixmyrtis* is configured for the *clear iproute* 192.168.116.16 EXEC mode command:

```
Router(config)#alias exec fixmyrt clear ip route 192.168.116.16
```

In the following example, the alias *express* is configured for the first part of the *access-expression* interface configuration command:

```
Router(config)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface e0
Router(config-if)#?
Interface configuration commands:
  access-expression Build a bridge boolean access expression
  .
  .
Router(config-if)#exit
```

```
Router(config)#alias ?
accept-dialin VPBN group accept dialin configuration mode
accept-dialout VPBN group accept dialout configuration mode
address-family Address Family configuration mode
call-discriminator Call Discriminator Configuration
cascustom Cas custom configuration mode
```
**clid-group** | CLID group configuration mode
---|---
**configure** | Global configuration mode
**congestion** | Frame Relay congestion configuration mode
**controller** | Controller configuration mode
**optone-set** | custom call progress tone configuration mode
**customer-profile** | customer profile configuration mode
**dhcp** | DHCP pool configuration mode
**dnis-group** | DNIS group configuration mode
**exec** | Exec mode
**flow-cache** | Flow aggregation cache config mode
**fr-fr** | FR/FR connection configuration mode
**interface** | Interface configuration mode

```
Router(config)# alias interface express access-expression
Router(config)# int e0
Router(config-if)# exp?
  *express=access-expression
Router(config-if)# express ?
    input Filter input packets
    output Filter output packets
!Note that the true form of the command/keyword alias appears on the screen after issuing the express ? command.
Router(config-if)# access-expression ?
    input Filter input packets
    output Filter output packets
Router(config-if)# ex?
  *express=access-expression exit
!Note that in the following line, a space is used before the ex? command so the alias is not displayed.
Router(config-if)# ex?
  exit
!Note that in the following line, the alias cannot be recognized because a space is used before the command.
Router#(config-if)# express ?
  % Unrecognized command
Router(config-if)# end
Router# show alias interface
Interface configuration mode aliases:
  express access-expression
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show aliases</strong></td>
<td>Displays command aliases.</td>
</tr>
</tbody>
</table>

### archive

To enter archive configuration mode, use the `archive` command in global configuration mode.

```
archive
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Archive configuration mode is not entered.

**Command Modes**

Global configuration (config)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to place the device in archive configuration mode:

```
Device# configure terminal
!
Device(config)# archive
Device(config-archive)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>log config</code></td>
<td>Enters configuration change logger configuration mode.</td>
</tr>
<tr>
<td><code>logging enable</code></td>
<td>Enables the logging of configuration changes.</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>path</code></td>
<td>Specifies the location and filename prefix for the files in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>time-period</code></td>
<td>Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.</td>
</tr>
</tbody>
</table>

### archive config

To save a copy of the current running configuration to the Cisco configuration archive, use the `archive config` command in privileged EXEC mode.

**archive config**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>
## Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Before using this command, you must configure the `path` command in order to specify the location and filename prefix for the files in the Cisco configuration archive.

The Cisco configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco configuration files to enhance the configuration rollback capability provided by the `configure replace` command. Before this feature was introduced, you could save copies of the running configuration using the `copy running-config destination-url` command, storing the target file either locally or remotely. However, this method lacked any automated file management. On the other hand, the Configuration Replace and Configuration Rollback feature provides the capability to automatically save copies of the running configuration to the Cisco configuration archive. These archived files serve as checkpoint configuration references and can be used by the `configure replace` command to revert to previous configuration states.

The `archive config` command allows you to save Cisco configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional time stamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved Cisco configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files has been saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The `show archive` command displays information for all configuration files saved in the Cisco configuration archive.

## Examples

The following example shows how to save the current running configuration to the Cisco configuration archive using the `archive config` command. Before using the `archive config` command, you must configure the `path` command to specify the location and filename prefix for the files in the Cisco IOS configuration archive. In this example, the location and filename prefix are specified as `disk0:myconfig` as follows:

```plaintext
configure terminal
!
archive
    path disk0:myconfig
end
```

You then save the current running configuration in the configuration archive, as follows:
The `show archive` command displays information on the files saved in the configuration archive as shown in the following sample output:

```
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
Archive #  Name
  0        
  1 disk0:myconfig<timestamp>-1
  2        
  3        
  4        
  5        
  6        
  7        
  8        
  9        
 10        
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td>configure confirm</td>
<td>Confirms replacement of the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td>configure replace</td>
<td>Replaces the current running configuration with a saved configuration file.</td>
</tr>
<tr>
<td>maximum</td>
<td>Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td>path</td>
<td>Specifies the location and filename prefix for the files in the Cisco configuration archive.</td>
</tr>
<tr>
<td>show archive</td>
<td>Displays information about the files saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td>time-period</td>
<td>Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.</td>
</tr>
</tbody>
</table>

### archive log config persistent save

To save the persisted commands in the configuration log to the Cisco IOS secure file system, use the `archive log config persistent save` command in privileged EXEC mode.

```
archive log config persistent save
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

If this command is not entered, the persisted configuration commands in the archive log are not saved to the Cisco IOS secure file system.
Command Modes
Privileged EXEC (#).

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

Usage Guidelines
If the router is in the persistent periodic mode, the persistent timer is restarted.

Examples
The following example saves the persisted commands in the archive log to the Cisco IOS secure file system:

```
Router# archive log config persistent save
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log config</td>
<td>Enters configuration change logger configuration mode.</td>
</tr>
<tr>
<td>logging enable</td>
<td>Enables the logging of configuration changes.</td>
</tr>
<tr>
<td>logging persistent</td>
<td>Enables the configuration logging persistent feature.</td>
</tr>
</tbody>
</table>

archive tar

To create a TAR file, to list files in a TAR file, or to extract the files from a TAR file, use the `archive tar` command in privileged EXEC mode.

```
archive tar [create destination-url flash:/file-url/table source-url/xtract source-url flash:/file-url [dir/file...]]
```
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>/create</strong></td>
<td>Creates a new TAR file on the local or network file system. For <code>destination-url</code>, specify the destination URL alias for the local or network file system and the name of the TAR file to create. The following options are supported:</td>
</tr>
<tr>
<td><code>destination-url</code></td>
<td>- <strong>flash</strong>: Syntax for the local flash file system.</td>
</tr>
<tr>
<td><code>flash:/ file-url</code></td>
<td>- <strong>ftp</strong>: <code>[[// username[: password}@ location]/ directory]/ tar-filename.tar</code> -- Syntax for FTP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>rcp</strong>: <code>[[// username@ location]/ directory]/ tar-filename.tar</code> -- Syntax for Remote Copy Protocol (RCP).</td>
</tr>
<tr>
<td></td>
<td>- <strong>tftp</strong>: <code>[[// location]/ directory]/ tar-filename.tar</code> -- Syntax for TFTP.</td>
</tr>
<tr>
<td>The <code>tar-filename.tar</code> is the name of the TAR file to be created. For <code>flash:/ file-url</code>, specify the location on the local flash file system from which the new TAR file is created. An optional list of files or directories within the source directory can be specified to write to the new TAR file. If none is specified, all files and directories at this level are written to the newly created TAR file.</td>
<td></td>
</tr>
<tr>
<td><strong>/table</strong></td>
<td>Display the contents of an existing TAR file to the screen. For <code>source-url</code>, specify the source URL alias for the local or network file system. The following options are supported:</td>
</tr>
<tr>
<td><code>source-url</code></td>
<td>- <strong>flash</strong>: Syntax for the local flash file system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ftp</strong>: <code>[[// username[: password}@ location]/ directory]/ tar-filename.tar</code> -- Syntax for FTP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>rcp</strong>: <code>[[// username@ location]/ directory]/ tar-filename.tar</code> -- Syntax for Remote Copy Protocol (RCP).</td>
</tr>
<tr>
<td></td>
<td>- <strong>tftp</strong>: <code>[[// location]/ directory]/ tar-filename.tar</code> -- Syntax for TFTP.</td>
</tr>
<tr>
<td>The <code>tar-filename.tar</code> is the name of the TAR file to be created.</td>
<td></td>
</tr>
<tr>
<td><strong>/xtract</strong></td>
<td>Extracts files from a TAR file to the local file system. For <code>source-url</code>, specify the source URL alias for the local file system. These options are supported:</td>
</tr>
<tr>
<td><code>source-url</code></td>
<td>- <strong>flash</strong>: Syntax for the local flash file system.</td>
</tr>
<tr>
<td><code>flash:/ file-url</code></td>
<td>- <strong>ftp</strong>: <code>[[// username[: password}@ location]/ directory]/ tar-filename.tar</code> -- Syntax for FTP.</td>
</tr>
<tr>
<td><code>[dir/file...]</code></td>
<td>- <strong>rcp</strong>: <code>[[// username@ location]/ directory]/ tar-filename.tar</code> -- Syntax for Remote Copy Protocol (RCP).</td>
</tr>
<tr>
<td></td>
<td>- <strong>tftp</strong>: <code>[[// location]/directory]/tar-filename.tar</code> -- Syntax for TFTP.</td>
</tr>
<tr>
<td>The <code>tar-filename.tar</code> is the name of the TAR file to be created.</td>
<td></td>
</tr>
</tbody>
</table>
async-bootp

To configure extended BOOTP requests for asynchronous interfaces as defined in RFC 1084, use the async-bootp command in global configuration mode. To restore the default, use the no form of this command.

async-bootp tag [hostname] data
no async-bootp
Syntax Description

<table>
<thead>
<tr>
<th>tag</th>
<th>Item being requested; expressed as filename, integer, or IP dotted decimal address. See the table below for possible keywords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>: hostname</td>
<td>(Optional) This entry applies only to the specified host. The :hostname argument accepts both an IP address and a logical host name.</td>
</tr>
<tr>
<td>data</td>
<td>List of IP addresses entered in dotted decimal notation or as logical host names, a number, or a quoted string.</td>
</tr>
</tbody>
</table>

**Table 5: tag Keyword Options**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootfile</td>
<td>Specifies use of a server boot file from which to download the boot program. Use the optional :hostname argument and the data argument to specify the filename.</td>
</tr>
<tr>
<td>subnet-mask mask</td>
<td>Dotted decimal address specifying the network and local subnetwork mask (as defined by RFC 950).</td>
</tr>
<tr>
<td>time-offset offset</td>
<td>Signed 32-bit integer specifying the time offset of the local subnetwork in seconds from Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>gateway address</td>
<td>Dotted decimal address specifying the IP addresses of gateways for this subnetwork. A preferred gateway should be listed first.</td>
</tr>
<tr>
<td>time-server address</td>
<td>Dotted decimal address specifying the IP address of time servers (as defined by RFC 868).</td>
</tr>
<tr>
<td>IEN116-server address</td>
<td>Dotted decimal address specifying the IP address of name servers (as defined by IEN 116).</td>
</tr>
<tr>
<td>nbns-server address</td>
<td>Dotted decimal address specifying the IP address of Windows NT servers.</td>
</tr>
<tr>
<td>DNS-server address</td>
<td>Dotted decimal address specifying the IP address of domain name servers (as defined by RFC 1034).</td>
</tr>
<tr>
<td>log-server address</td>
<td>Dotted decimal address specifying the IP address of an MIT-LCS UDP log server.</td>
</tr>
<tr>
<td>quote-server address</td>
<td>Dotted decimal address specifying the IP address of Quote of the Day servers (as defined in RFC 865).</td>
</tr>
<tr>
<td>lpr-server address</td>
<td>Dotted decimal address specifying the IP address of Berkeley UNIX Version 4 BSD servers.</td>
</tr>
<tr>
<td>impress-server address</td>
<td>Dotted decimal address specifying the IP address of Impress network image servers.</td>
</tr>
<tr>
<td>rlp-server address</td>
<td>Dotted decimal address specifying the IP address of Resource Location Protocol (RLP) servers (as defined in RFC 887).</td>
</tr>
<tr>
<td>hostname name</td>
<td>The name of the client, which may or may not be domain qualified, depending upon the site.</td>
</tr>
</tbody>
</table>
### async-bootp

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootfile-size</td>
<td>A two-octet value specifying the number of 512-octet (byte) blocks in the default boot file.</td>
</tr>
</tbody>
</table>

#### Command Default

If no extended BOOTP commands are entered, the Cisco IOS software generates a gateway and subnet mask appropriate for the local network.

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the `show async-bootp` EXEC command to list the configured parameters. Use the `no async-bootp` command to clear the list.

#### Examples

The following example illustrates how to specify different boot files: one for a PC, and one for a Macintosh. With this configuration, a BOOTP request from the host on 172.30.1.1 results in a reply listing the boot filename as `pcboot`. A BOOTP request from the host named “mac” results in a reply listing the boot filename as “macboot.”

```
async-bootp bootfile :172.30.1.1 "pcboot"
async-bootp bootfile :mac "macboot"
```

The following example specifies a subnet mask of 255.255.0.0:

```
async-bootp subnet-mask 255.255.0.0
```

The following example specifies a negative time offset of the local subnetwork of 3600 seconds:

```
async-bootp time-offset -3600
```

The following example specifies the IP address of a time server:

```
async-bootp time-server 172.16.1.1
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show async bootp</code></td>
<td>Displays the extended BOOTP request parameters that have been configured for asynchronous interfaces.</td>
</tr>
</tbody>
</table>

#### attach

To connect to a specific line card or module from a remote location for the purpose of executing monitoring and maintenance commands on that line card or module, use the `attach` command in privileged EXEC mode.
To exit from the Cisco IOS software image on the line card and return to the Cisco IOS image on the main (Supervisor) module, use the `exit` command.

**Cisco 12000 Series**

```
attach  slot-number
```

**Cisco 7600 Series and Catalyst 6500 Series**

```
attach  module-number
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>slot-number</code></td>
<td>Slot number of the line card to which you wish to connect. If you omit the slot number, you will be prompted for it.</td>
</tr>
<tr>
<td><code>module-number</code></td>
<td>Module number; see the “Usage Guidelines” section for valid values.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2GS</td>
<td>This command was introduced on the Cisco 12000 series.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support was added for the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Cisco 12000 Series**

You must first use the `attach` privileged EXEC command to access the Cisco IOS software image on a line card before using line card-specific `show` EXEC commands. Alternatively, you can use the `execute-on` privileged EXEC command to execute a `show` command on a specific line card.

After you connect to the Cisco IOS image on the line card using the `attach` command, the prompt changes to `LC-Slotx#`, where `x` is the slot number of the line card.

The commands executed on the line card use the Cisco IOS image on that line card.

You can also use the `execute-on slot` privileged EXEC command to execute commands on one or all line cards.

**Note**

Do not execute the `config` EXEC command from the Cisco IOS software image on the line card.

**Cisco 7600 Series and Catalyst 6500 Series**

**Caution**

After you enter the `attach` or `remote login` command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.
The valid values for the `module-number` argument depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

This command is supported on Distributed Forwarding Card (DFC)-equipped modules, FlexWan modules, and the supervisor engine only.

When you execute the `attach module-number` command, the prompt changes to `Router-dfcx#` or `Switch-sp#`, depending on the type of module to which you are connecting.

The behavior of the `attach` command is identical to that of the `remote login module num` command.

There are two ways to end this session:

- You can enter the `exit` command as follows:

```
Router-dfc3# exit
[Connection to Switch closed by foreign host]
Router#
```

- You can press Ctrl-C three times as follows:

```
Router-dfc3# ^C
Router-dfc3# ^C
Router-dfc3# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

### Examples

In the following example, the user connects to the Cisco IOS image running on the line card in slot 9, gets a list of valid `show` commands, and returns the Cisco IOS image running on the GRP:

```
Router# attach 9
Entering Console for 4 Port Packet Over SONET OC-3c/STM-1 in Slot: 9
Type exit to end this session
Press RETURN to get started!
LC-Slot9# show ?
    cef Cisco Express Forwarding
    clock Display the system clock
    context Show context information about recent crash(s)
    history Display the session command history
    hosts IP domain-name, lookup style, nameservers, and host table
    ipc Interprocess communications commands
    location Display the system location
    sessions Information about Telnet connections
    terminal Display terminal configuration parameters
    users Display information about terminal lines
    version System hardware and software status
LC-Slot9# exit
Disconnecting from slot 9.
Connection Duration: 00:01:04
Router#
```

### Note

Because not all statistics are maintained on line cards, the output from some of `show` commands may be inconsistent.

The following example shows how to log in remotely to the DFC-equipped module:
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach shelf</td>
<td>Connects you to a specific (managed) shelf for the purpose of remotely executing commands on that shelf only.</td>
</tr>
<tr>
<td>execute-on slot</td>
<td>Executes commands remotely on a specific line card, or on all line cards simultaneously.</td>
</tr>
<tr>
<td>remote login</td>
<td>Accesses the Cisco 7600 series router console or a specific module.</td>
</tr>
</tbody>
</table>

autobaud

To set the line for automatic baud rate detection (autobaud), use the `autobaud` command in line configuration mode. To disable automatic baud detection, use the `no` form of this command.

`autobaud`
`no autobaud`

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Autobaud detection is disabled. Fixed speed of 9600 bps.

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The autobaud detection supports a range from 300 to 19200 baud. A line set for autobaud cannot be used for outgoing connections, nor can you set autobaud capability on a line using 19200 baud when the parity bit is set (because of hardware limitations).

**Note**

Automatic baud detection must be disabled by using the `no autobaud` command prior to setting the txspeed, rxspeed, or speed commands.

**Examples**

In the following example, the auxiliary port is configured for autobaud detection:

```
Router(config)# line aux
```
auto-sync

To enable automatic synchronization of the configuration files in NVRAM, use the **auto-sync** command in main-cpu redundancy configuration mode. To disable automatic synchronization, use the **no** form of this command.

```
auto-sync {startup-config|config-register|bootvar|running-config|standard}
no auto-sync {startup-config|config-register|bootvar|standard}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Specifies synchronization of the startup configuration files.</td>
</tr>
<tr>
<td>config-register</td>
<td>Specifies synchronization of the configuration register values.</td>
</tr>
<tr>
<td>bootvar</td>
<td>Specifies synchronization of the following boot variables:</td>
</tr>
<tr>
<td></td>
<td>• BOOT--Set by the <strong>boot system</strong> <code>device:filename</code> command.</td>
</tr>
<tr>
<td></td>
<td>• CONFIG_FILE--Set by the <strong>boot config</strong> <code>device:filename</code> command.</td>
</tr>
<tr>
<td>running-config</td>
<td>Specifies synchronization of the running configuration files.</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies synchronization of all of the system files (startup configuration, boot variables, and config configuration registers).</td>
</tr>
</tbody>
</table>

**Command Default**

For the Performance Routing Engines (PREs) on the Cisco uBR10012 universal broadband router, the system defaults to synchronizing all system files on the (**auto-sync standard**).

For the Supervisor Engines on the Cisco 7600 series routers, the system defaults to synchronizing the running configuration (**running-config**).

At the Cisco RF Gateway 10 chassis level, all the system files are synchronized by default.

**Command Modes**

Redundancy configuration (config-r)

Main CPU redundancy configuration (config-r-mc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)XF1</td>
<td>This command was introduced on the Cisco uBR10012 universal broadband router.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support was added for the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>Support for this command on the Cisco 7600 series routers was removed.</td>
</tr>
<tr>
<td>12.3BC</td>
<td>This command was integrated into Cisco IOS Release 12.3BC for the Cisco uBR10012 router.</td>
</tr>
<tr>
<td>12.2(33)SCA</td>
<td>This command is obsolete on the Cisco uBR10012 universal broadband router.</td>
</tr>
<tr>
<td>12.2(44)SQ</td>
<td>This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Cisco 7600 Series Routers

If you enter the no auto-sync standard command, no automatic synchronizations occur. If you want to enable any of the keywords, you have to enter the appropriate command for each keyword.

The auto-sync command is not supported in RPR+ mode.

Cisco uBR10012 Universal Broadband Router

By default, the system synchronizes all system files, which is the typical setting for most applications. However, you might want to exclude certain files from synchronization for specialized applications.

For example, if you have configured the active and standby PRE1 (or PRE2) modules to run different versions of Cisco IOS software, you might want to use different configuration files as well. In this case, you would not synchronize the startup configuration file.

Cisco RF Gateway 10

We recommend that you use the auto-sync standard command to ensure that all system files are synchronized between the two Supervisor modules. The no auto-sync command is not used in production plants.

Examples

Cisco 7600 Series Routers

The following example shows how (from the default configuration) to enable automatic synchronization of the configuration register in the main CPU:

```
Router# configure terminal
Router (config)# redundancy
Router (config-r)# main-cpu
Router (config-r-cpu)#
no auto-sync standard
Router (config-r-cpu)# auto-sync config-register
```
Cisco uBR10012 Universal Broadband Router

The following example shows the system being configured to synchronize only the startup configuration file:

```
router(config)# redundancy
router(config-r)# main-cpu
router(config-r-mc)# auto-sync startup-config
router(config-r-mc)# exit

router(config-r)# exit
```

The following example shows how to configure the system to synchronize all system files except for the startup configuration file. This typically is done when the two PRE1 (or PRE2) modules are running different software images.

```
router(config)# redundancy
router(config-r)# main-cpu
router(config-r-mc)# no auto-sync startup-config
router(config-r-mc)# auto-sync config-register
router(config-r-mc)# auto-sync bootvar
router(config-r-mc)# exit

router(config-r)# exit
```

Cisco RF Gateway 10

The following example shows the synchronization of all system files on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-r-mc)# auto-sync standard
Router(config-r-mc)# exit
Router(config-red)# exit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy</td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td>main-cpu</td>
<td>Enters main CPU redundancy configuration mode.</td>
</tr>
</tbody>
</table>

### autoupgrade disk-clean-up

To configure the Cisco IOS Auto-Upgrade Manager disk cleanup utility, use the `autoupgrade disk-clean-up` command in global configuration mode. To disable this configuration, use the `no` form of this command.

```
autoupgrade disk-clean-up [{crashinfo|core|image|irrecoverable}]
no autoupgrade disk-clean-up [{crashinfo|core|image|irrecoverable}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo</td>
<td>(Optional) Deletes crashinfo files during disk-clean-up before an image is downloaded.</td>
</tr>
</tbody>
</table>
autoupgrade ida url

By default, the crashinfo files, the core files, and the Cisco software images are deleted by the Cisco IOS Auto-Upgrade Manager disk cleanup utility, and the filesystems that support the undelete operation are not cleaned up.

Command Modes
Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to clean-up filesystems that support undelete operation:

Device(config)# autoupgrade disk-cleanup irrecoverable

The following example shows how to avoid deleting the Cisco software images:

Device(config)# no autoupgrade disk-cleanup image

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoupgrade ida url</td>
<td>Configures the URL of the server on <a href="http://www.cisco.com">www.cisco.com</a> where the image download requests will be sent by the Cisco IOS Auto-Upgrade Manager.</td>
</tr>
<tr>
<td>autoupgrade status email</td>
<td>Configures the address to which the status email is to be sent.</td>
</tr>
<tr>
<td>upgrade automatic getversion</td>
<td>Downloads a Cisco software image directly from <a href="http://www.cisco.com">www.cisco.com</a> or from a non-Cisco server.</td>
</tr>
</tbody>
</table>

autoupgrade ida url

To configure the URL of the Intelligent Download Application (IDA) running on www.cisco.com, use the autoupgrade ida url command in global configuration mode. To disable this URL, use the no form of this command.

autoupgrade ida url  
no autoupgrade ida url

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>URL of the IDA server.</td>
</tr>
</tbody>
</table>
**autoupgrade status email**

To configure the address to which status email is to be sent and the outgoing email server, use the `autoupgrade status email` command in global configuration mode. To disable status email, use the `no` form of this command.

```
autoupgrade status email [recipient [email-address]] [smtp-server [smtp-server]]
no autoupgrade status email [recipient [email-address]] [smtp-server [smtp-server]]
```

**Syntax Description**

- **recipient**
  - The address to which the Cisco IOS Auto-Upgrade Manager (AUM) status is to be sent.

- **smtp-server**
  - The outgoing email server to which the AUM email is sent.

- **email-address**
  - The email address to which the AUM status is to be sent.

**Command Default**

Status email is not sent unless the address is configured. The recipient email address and SMTP server have to be configured in order to receive AUM status email.

**Command Modes**

Global configuration (config)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to configure the email-address where AUM status email can be sent.

### Examples

The following example shows how to configure the address to which status email is to be sent:

```
Device(config)# autoupgrade status email recipient tree@abc.com
Device(config)# autoupgrade status email smtp-server smtpserver.abc.com
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoupgrade disk-cleanup</td>
<td>Configures the Cisco IOS Auto-Upgrade Manager disk cleanup utility.</td>
</tr>
<tr>
<td>autoupgrade ida url</td>
<td>Configures the URL of the server running on <a href="http://www.cisco.com">www.cisco.com</a> to which the device sends the image download requests.</td>
</tr>
<tr>
<td>upgrade automatic getversion</td>
<td>Downloads a Cisco software image directly from <a href="http://www.cisco.com">www.cisco.com</a> or from a non-Cisco server.</td>
</tr>
</tbody>
</table>

### banner exec

To specify and enable a message to be displayed when an EXEC process is created (an EXEC banner), use the `banner exec` command in global configuration mode. To delete the existing EXEC banner, use the `no` form of this command.

```
banner exec d message d
no banner exec
```

#### Syntax Description

<table>
<thead>
<tr>
<th>d</th>
<th>Delimiting character of your choice--a pound sign (#), for example. You cannot use the delimiting character in the banner message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>Message text. You can include tokens in the form ${token}$ in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in the table below.</td>
</tr>
</tbody>
</table>

#### Command Default

Disabled (no EXEC banner is displayed).

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(7.5)AA</td>
<td>Token functionality was introduced.</td>
</tr>
</tbody>
</table>
Modification

Release    Modification
12.0(3)T   Token functionality was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command specifies a message to be displayed when an EXEC process is created (a line is activated, or an incoming connection is made to a vty). Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a router, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

To disable the EXEC banner on a particular line or lines, use the \texttt{no exec-banner} line configuration command.

To customize the banner, use tokens in the form \texttt{$(token)$} in the message text. Tokens will display current Cisco IOS configuration variables, such as the router’s host name and IP address. The tokens are described in the table below.

\textbf{Table 6: banner exec Tokens}

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{(hostname)}$</td>
<td>Displays the host name for the router.</td>
</tr>
<tr>
<td>$\text{(domain)}$</td>
<td>Displays the domain name for the router.</td>
</tr>
<tr>
<td>$\text{(line)}$</td>
<td>Displays the vty or tty (asynchronous) line number.</td>
</tr>
<tr>
<td>$\text{(line-desc)}$</td>
<td>Displays the description attached to the line.</td>
</tr>
</tbody>
</table>

Examples

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Notice that the $\text{(token)}$ syntax is replaced by the corresponding configuration variable.

```
Router(config)# banner exec %
Enter TEXT message. End with the character '%'.
Session activated on line $(line), $(line-desc). Enter commands at the prompt. %
```

When a user logs on to the system, the following output is displayed:

```
User Access Verification
Username: joeuser
Password: <password>
Session activated on line 50, vty default line. Enter commands at the prompt.
Router>
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner incoming</td>
<td>Defines a customized banner to be displayed when there is an incoming connection to a terminal line from a host on the network.</td>
</tr>
<tr>
<td>banner login</td>
<td>Defines a customized banner to be displayed before the username and password login prompts.</td>
</tr>
<tr>
<td>banner motd</td>
<td>Defines a customized message-of-the-day banner.</td>
</tr>
<tr>
<td>banner slip-ppp</td>
<td>Defines a customized banner to be displayed when a serial-line IP or point-to-point connection is made.</td>
</tr>
<tr>
<td>exec-banner</td>
<td>Controls (enables or disables) the display of EXEC banners and message-of-the-day banners on a specified line or lines.</td>
</tr>
</tbody>
</table>

banner incoming

To define and enable a banner to be displayed when there is an incoming connection to a terminal line from a host on the network, use the `banner incoming` command in global configuration mode. To delete the incoming connection banner, use the `no` form of this command.

```
banner incoming d message d
no banner incoming
```

Syntax Description

- `d` | Delimiting character of your choice--a pound sign (#), for example. You cannot use the delimiting character in the banner message.
- `message` | Message text. You can include tokens in the form `$token` in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in the table below.

Command Default

Disabled (no incoming banner is displayed).

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(7.5)AA</td>
<td>Token functionality was introduced.</td>
</tr>
<tr>
<td>12.0(3)T</td>
<td>Token functionality was integrated into Cisco IOS Release 12.0(3)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Follow the `banner incoming` command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

An incoming connection is one initiated from the network side of the router. Incoming connections are also called reverse Telnet sessions. These sessions can display MOTD banners and incoming banners, but they do
not display EXEC banners. Use the **no motd-banner** line configuration command to disable the MOTD banner for reverse Telnet sessions on asynchronous lines.

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, before the login prompt. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

Incoming banners cannot be suppressed. If you do not want the incoming banner to appear, you must delete it with the **no banner incoming** command.

To customize the banner, use tokens in the form `$\{token\}$` in the message text. Tokens will display current Cisco IOS configuration variables, such as the router’s host name and IP address. The tokens are described in the table below.

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>${hostname}$</td>
<td>Displays the host name for the router.</td>
</tr>
<tr>
<td>${domain}$</td>
<td>Displays the domain name for the router.</td>
</tr>
<tr>
<td>${line}$</td>
<td>Displays the vty or tty (asynchronous) line number.</td>
</tr>
<tr>
<td>${line-desc}$</td>
<td>Displays the description attached to the line.</td>
</tr>
</tbody>
</table>

**Examples**

The following example sets an incoming connection banner. The pound sign (`#`) is used as a delimiting character.

```
Router(config)# banner incoming #
This is the Reuses router.
#
```

The following example sets an incoming connection banner that uses several tokens. The percent sign (`%`) is used as a delimiting character.

```
darkstar(config)# banner incoming %
Enter TEXT message. End with the character '%'.
You have entered $\{hostname\}.$\{domain\} on line $\{line\} ($\{line-desc\}) %
```

When the incoming connection banner is executed, the user will see the following banner. Notice that the `$\{token\}$` syntax is replaced by the corresponding configuration variable.

```
You have entered darkstar.ourdomain.com on line 5 (Dialin Modem)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner exec</td>
<td>Defines a customized banner to be displayed whenever the EXEC process is initiated.</td>
</tr>
<tr>
<td>banner login</td>
<td>Defines a customized banner to be displayed before the username and password login prompts.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>banner motd</em></td>
<td>Defines a customized message-of-the-day banner.</td>
</tr>
<tr>
<td><em>banner slip-ppp</em></td>
<td>Defines a customized banner to be displayed when a serial-line IP or point-to-point connection is made.</td>
</tr>
</tbody>
</table>

### banner login

To define and enable a customized banner to be displayed before the username and password login prompts, use the *banner login* command in global configuration mode. To disable the login banner, use *no* form of this command.

**Syntax**

*banner login* `d` *message* `d`

*no banner login*

**Syntax Description**

| `d` | Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message. |
| `message` | Message text. You can include tokens in the form $\{token\}$ in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in the table below. |

**Command Default**

Disabled (no login banner is displayed).

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(7.5)AA</td>
<td>Token functionality was introduced.</td>
</tr>
<tr>
<td>12.0(3)T</td>
<td>Token functionality was integrated into Cisco IOS Release 12.0(3)T.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Follow the *banner login* command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

To customize the banner, use tokens in the form $\{token\}$ in the message text. Tokens will display current Cisco IOS configuration variables, such as the router’s host name and IP address. The tokens are described in the table below.
Table 8: banner login Tokens

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(hostname)</td>
<td>Displays the host name for the router.</td>
</tr>
<tr>
<td>$(domain)</td>
<td>Displays the domain name for the router.</td>
</tr>
<tr>
<td>$(line)</td>
<td>Displays the vty or tty (asynchronous) line number.</td>
</tr>
<tr>
<td>$(line-desc)</td>
<td>Displays the description attached to the line.</td>
</tr>
</tbody>
</table>

Examples

The following example sets a login banner. Double quotes (") are used as the delimiting character.

Router# banner login " Access for authorized users only. Please enter your username and password. "

The following example sets a login banner that uses several tokens. The percent sign (%) is used as the delimiting character.

darkstar(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain) on line $(line) ($(line-desc)) %

When the login banner is executed, the user will see the following banner. Notice that the $(token) syntax is replaced by the corresponding configuration variable.

You have entered darkstar.ourdomain.com on line 5 (Dialin Modem)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner exec</td>
<td>Defines a customized banner to be displayed whenever the EXEC process is initiated.</td>
</tr>
<tr>
<td>banner incoming</td>
<td>Defines a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.</td>
</tr>
<tr>
<td>banner motd</td>
<td>Defines a customized message-of-the-day banner.</td>
</tr>
<tr>
<td>banner slip-ppp</td>
<td>Defines a customized banner to be displayed when a serial-line IP or point-to-point connection is made.</td>
</tr>
</tbody>
</table>

banner motd

To define and enable a message-of-the-day (MOTD) banner, use the **banner motd** command in global configuration mode. To delete the MOTD banner, use the **no** form of this command.

banner motd  
no banner motd
**Syntax Description**

<table>
<thead>
<tr>
<th>Delimiting character of your choice--a pound sign (#), for example. You cannot use the delimiting character in the banner message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message text. You can include tokens in the form $(token)$ in the message text. Tokens will be replaced with the corresponding configuration variable.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled (no MOTD banner is displayed).

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(7.5)AA</td>
<td>Token functionality was introduced.</td>
</tr>
<tr>
<td>12.0(3)T</td>
<td>Token functionality was integrated into Cisco IOS Release 12.0(3)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

This MOTD banner is displayed to all terminals connected and is useful for sending messages that affect all users (such as impending system shutdowns). Use the `no exec-banner` or `no motd-banner` command to disable the MOTD banner on a line. The `no exec-banner` command also disables the EXEC banner on the line.

When a user connects to the router, the MOTD banner appears before the login prompt. After the user logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

To customize the banner, use tokens in the form $(token)$ in the message text. Tokens will display current Cisco IOS configuration variables, such as the router’s host name and IP address. The tokens are described in the table below.

**Table 9: banner motd Tokens**

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(hostname)</td>
<td>Displays the host name for the router.</td>
</tr>
<tr>
<td>$(domain)</td>
<td>Displays the domain name for the router.</td>
</tr>
<tr>
<td>$(line)</td>
<td>Displays the vty or tty (asynchronous) line number.</td>
</tr>
<tr>
<td>$(line-desc)</td>
<td>Displays the description attached to the line.</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures an MOTD banner. The pound sign (#) is used as a delimiting character.
Router# banner motd # Building power will be off from 7:00 AM until 9:00 AM this coming Tuesday.

The following example configures an MOTD banner with a token. The percent sign (%) is used as a delimiting character.

darkstar(config)# banner motd %
Enter TEXT message. End with the character '%'.
Notice: all routers in $(domain) will be upgraded beginning April 20 %

When the MOTD banner is executed, the user will see the following. Notice that the $(token) syntax is replaced by the corresponding configuration variable.

Notice: all routers in ourdomain.com will be upgraded beginning April 20

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>banner exec</td>
<td>Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.</td>
</tr>
<tr>
<td></td>
<td>banner incoming</td>
<td>Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.</td>
</tr>
<tr>
<td></td>
<td>banner login</td>
<td>Defines and enables a customized banner to be displayed before the username and password login prompts.</td>
</tr>
<tr>
<td></td>
<td>banner slip-ppp</td>
<td>Defines and enables a customized banner to be displayed when a serial-line IP or point-to-point connection is made.</td>
</tr>
<tr>
<td></td>
<td>exec-banner</td>
<td>Controls (enables or disables) the display of EXEC banners and message-of-the-day banners on a specified line or lines.</td>
</tr>
<tr>
<td></td>
<td>motd-banner</td>
<td>Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.</td>
</tr>
</tbody>
</table>

**banner slip-ppp**

To customize the banner that is displayed when a Serial Line Internet Protocol (SLIP) or PPP connection is made, use the **banner slip-ppp** command in global configuration mode. To restore the default SLIP or PPP banner, use the **no** form of this command.

```
banner slip-ppp d message d
no banner slip-ppp
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d$</td>
<td>Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.</td>
</tr>
<tr>
<td>message</td>
<td>Message text. You can include tokens in the form $(token)$ in the message text. Tokens will be replaced with the corresponding configuration variable.</td>
</tr>
</tbody>
</table>
The default SLIP or PPP banner message is:

```
Entering encapsulation mode.
Async interface address is unnumbered (Ethernet0)
Your IP address is 10.000.0.0 MTU is 1500 bytes
```

The banner message when using the service old-slip-prompt command is:

```
Entering encapsulation mode.
Your IP address is 10.100.0.0 MTU is 1500 bytes
```

where encapsulation is SLIP or PPP.

### Command Modes

#### Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use this command to define a custom SLIP or PPP connection message. This is useful when legacy client applications require a specialized connection string. To customize the banner, use tokens in the form \$\{token\} in the message text. Tokens will display current Cisco IOS configuration variables, such as the routers host name, IP address, encapsulation type, and Maximum Transfer Unit (MTU) size. The banner tokens are described in the table below.

### Table 10: banner slip-ppp Tokens

<table>
<thead>
<tr>
<th>Token</th>
<th>Information Displayed in the Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(hostname)</td>
<td>Displays the host name of the router.</td>
</tr>
<tr>
<td>$(domain)</td>
<td>Displays the domain name of the router.</td>
</tr>
<tr>
<td>$(peer-ip)</td>
<td>Displays the IP address of the peer machine.</td>
</tr>
<tr>
<td>$(gate-ip)</td>
<td>Displays the IP address of the gateway machine.</td>
</tr>
<tr>
<td>$(encap)</td>
<td>Displays the encapsulation type (SLIP, PPP, and so on).</td>
</tr>
<tr>
<td>$(encap-alt)</td>
<td>Displays the encapsulation type as SL/IP instead of SLIP.</td>
</tr>
<tr>
<td>$(mtu)</td>
<td>Displays the MTU size.</td>
</tr>
</tbody>
</table>

### Examples

The following example sets the SLIP/PPP banner using several tokens and the percent sign (%) as the delimiting character:

```bash
Router(config)# banner slip-ppp %
Enter TEXT message. End with the character '%%'.
```
Starting $(encap)$ connection from $(gate-ip)$ to $(peer-ip)$ using a maximum packet size of $(mtu)$ bytes... %

The new SLIP/PPP banner will now be displayed when the slip EXEC command is used. Notice that the $(token)$ syntax is replaced by the corresponding configuration variable.

Router# slip
Starting SLIP connection from 172.16.69.96 to 192.168.1.200 using a maximum packet size of 1500 bytes...

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner exec</td>
<td>Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.</td>
</tr>
<tr>
<td>banner incoming</td>
<td>Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.</td>
</tr>
<tr>
<td>banner motd</td>
<td>Defines and enables a customized message-of-the-day banner.</td>
</tr>
<tr>
<td>ppp</td>
<td>Initiates a connection to a remote host using PPP.</td>
</tr>
<tr>
<td>slip</td>
<td>Initiates a connection to a remote host using SLIP.</td>
</tr>
</tbody>
</table>

### boot

To boot the router manually, use the `boot` command in ROM monitor mode. The syntax of this command varies according to the platform and ROM monitor version.

- **boot**
- **boot** `file-url`
- **boot** `filename` [tftp-ip-address]
- **boot** `flash` `[flash-fs:]][partition-number:][filename]`

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>file-url</code></td>
<td>URL of the image to boot (for example, <code>boot tftp://172.16.15.112/routertest</code>).</td>
</tr>
</tbody>
</table>
filename | When used in conjunction with the `ip-address` argument, the `filename` argument is the name of the system image file to boot from a network server. The filename is case sensitive. When used in conjunction with the `flash` keyword, the `filename` argument is the name of the system image file to boot from Flash memory. On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, the system obtains the image file from internal Flash memory. On the Cisco 1600 series, Cisco 3600 series and Cisco 7000 family routers, the `flash-fs` argument specifies the Flash memory device from which to obtain the system image. (See the `flash-fs` argument later in this table for valid device values.) The filename is case sensitive. Without the `filename` argument, the first valid file in Flash memory is loaded. If the `filename` is not specified, the first file in the partition or file system is used. (A USB Flash uses the first image in (compact) Flash as the boot loader and loads the image from USB Flash.)

| tftp-ip-address | (optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

| flash | Boots the router from Flash memory. Note that this keyword is required in some boot images.

| usbflash0 | Boot the first file in USB Flash 0. If the optional `filename` argument is used, the router boots the specified image from USB Flash.

| Note | This option uses the first image in (compact) Flash as the boot loader and loads the image from USB Flash.

| flash-fs : | (Optional) Specifying the Flash file system is optional for all platforms except the Cisco 7500 series routers. Possible file systems are:

- flash: --Internal Flash memory.

- bootflash: --Internal Flash memory on the Cisco 7000 family.

- slot0: --Flash memory card in the first PCMCIA slot on the Cisco 7000 family and Cisco 3600 series routers.

- slot1: --Flash memory card in the second PCMCIA slot on the Cisco 7000 family and Cisco 3600 series routers.

| partition-number : | (Optional) Specifies the partition number of the file system the file should be loaded from. This argument is not available on all platforms. If the `partition-number` is not specified, the first partition is used.

---

**Command Default**

For most platforms, if you enter the `boot` command and press Enter, the router boots from ROM by default. However, for some platforms, such as the Cisco 3600 series routers, if you enter the `boot` command and press Enter, the router boots the first image in Flash memory. Refer to the documentation for your platform for information about the default image.

**Command Modes**

ROM monitor
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The usbflash0 keyword was added to support booting an image from an external USB Flash drive.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To determine which form of this command to use, refer to the documentation for your platform or use the CLI help (?) feature.

Use this command only when your router cannot find the boot configuration information needed in NVRAM. To enter ROM monitor mode, use one of the following methods:

- Enter the `reload` EXEC command, then press the Break key during the first 60 seconds of startup.
- Set the configuration register bits 0 to 3 to zero (for example, set the configuration register to 0x0) and enter the `reload` command.

The ROM Monitor prompt is either “>” or, for newer platforms, “rommon x >”. Enter only lowercase commands.

These commands work only if there is a valid image to boot. Also, from the ROM monitor prompt, issuing a prior reset command is necessary for the boot to be consistently successful.

In Cisco IOS Release 12.3(4)T, MONLIB was modified to search in media for a valid Cisco IOS image. This change prevents boot failures that result when the first file read in disk or flash is not a valid Cisco IOS image. Refer to your hardware documentation for information on correct jumper settings for your platform.

**Note**

For some platforms the `flash` keyword is now required. If your attempts to use the boot command are failing using the older `boot flash:\[filename\]` syntax, try using the `boot flash flash:\[filename\]` syntax.

**Examples**

In the following example, a router is manually booted from ROM:

```
> boot
F3: (ROM Monitor copyrights)
```

In the following example, a router boots the file named routertest from a network server with the IP address 172.16.15.112 using the `file-url` syntax:

```
> boot tftp://172.16.15.112/routertest
F3: (ROM Monitor copyrights)
```

The following example shows the `boot flash` command without the `filename` argument. The first valid file in Flash memory is loaded.

```
> boot flash
F3: 1858656+45204+166896 at 0x1000
Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
```
The following example boots from Flash memory using the file named gs7-k:

```bash
> boot flash gs7-k
F3: 1858676+45204+166896 at 0x1000
Booting gs7-k from flash memory
F3: 1858676+45204+166896 at 0x1000
(ROM Monitor copyrights)
```

In the following example, the `boot flash flash:` command boots the relocatable image file named igs-bpx-l from partition 2 in Flash memory:

```bash
> boot flash flash:2:igs-bpx-l
F3: 3562264+98228+303632 at 0x30000B4
(ROM Monitor copyrights)
```

In the following command, the Cisco 7000 family router accepts the `flash` keyword for compatibility but ignores it, and boots from slot 0:

```bash
> boot flash slot0:gs7-k-mz.103-9
F3: 8468+3980384+165008 at 0x1000
```

In the following example, the command did not function because it must be entered in lowercase:

```bash
rommon 10 > BOOT
command "BOOT" not found
```

The following example boots the first file in the first partition of internal Flash memory of a Cisco 3600 series router:

```bash
> boot flash:
```

The following example boots the first image file in the first partition of the Flash memory card in slot 0 of a Cisco 3600 series router:

```bash
> boot slot0:
```

The following example shows the ROM monitor booting the first file in the first Flash memory partition on a Cisco 1600 series router:

```bash
> boot flash:
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>continue</td>
<td>Returns to EXEC mode from ROM monitor mode by completing the boot process.</td>
</tr>
</tbody>
</table>
Related Topics
- boot bootldr, on page 40
- boot bootstrap, on page 41
- boot config, on page 43
- boot host, on page 45

**boot bootldr**

To specify the location of the boot image that ROM uses for booting, use the `boot bootldr` command in global configuration mode. To remove this boot image specification, use the `no` form of this command.

```
boot bootldr file-url
no boot bootldr
```

**Syntax Description**
- **file-url**: URL of the boot image on a Flash file system.

**Command Default**
Refer to your platform documentation for the location of the default boot boot image.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `boot bootldr` command sets the BOOTLDR variable in the current running configuration. You must specify both the Flash file system and the filename.

**Note**
When you use this global configuration command, you affect only the running configuration. You must save the variable setting to your startup configuration to place the information under ROM monitor control and to have the variable function as expected. Use the `copy system:running-config nvram:startup-config` command to save the variable from your running configuration to your startup configuration.

**Note**
The default length of the bootstrap filename is 64 characters. Depending on the platform a longer bootstrap filename can be used and supported.

The `no` form of the command sets the BOOTLDR variable to a null string. On the Cisco 7000 family routers, a null string causes the first image file in boot Flash memory to be used as the boot image that ROM uses for booting.

Use the `show boot` command to display the current value for the BOOTLDR variable.

**Examples**

In the following example, the internal Flash memory contains the boot image:
The following example specifies that the Flash memory card inserted in slot 0 contains the boot image:

```plaintext
boot bootldr slot0:boot-image
```

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy system:running-config nvram:startup-config</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>show (flash file system)</td>
<td>Displays the layout and contents of a Flash memory file system.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting.</td>
</tr>
</tbody>
</table>

---

### boot bootstrap

To configure the filename that is used to boot a secondary bootstrap image, use the `boot bootstrap` command in global configuration mode. To disable booting from a secondary bootstrap image, use the `no` form of this command.

```plaintext
boot bootstrap file-url
no boot bootstrap file-url
boot bootstrap flash [filename]
no boot bootstrap flash [filename]
boot bootstrap [tftp] filename [ip-address]
no boot bootstrap [tftp] filename [ip-address]
boot bootstrap mop filename [interface-type interface-number]
no boot bootstrap mop filename [interface-type interface-number]
```

---

### Syntax Description

<table>
<thead>
<tr>
<th>file-url</th>
<th>URL of the bootstrap image.</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>Boots the router from flash memory.</td>
</tr>
<tr>
<td>filename</td>
<td>(Optional with <code>flash</code>) Name of the system image to boot from a network server or from flash memory. If you omit the filename when booting from flash memory, the router uses the first system image stored in flash memory.</td>
</tr>
<tr>
<td>tftp</td>
<td>(Optional) Boots the router from a system image stored on a TFTP server.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(Optional) IP address of the TFTP server on which the system image resides. If the <code>ip-address</code> argument is omitted, this value defaults to the IP broadcast address of 255.255.255.255.</td>
</tr>
<tr>
<td>mop</td>
<td>Boots the router from a DECnet Maintenance Operation Protocol (MOP) server.</td>
</tr>
</tbody>
</table>
### Command Default

No secondary bootstrap is configured.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The mop keyword and interface-type interface-number arguments were added.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **boot bootstrap** command causes the router to load a secondary bootstrap image from the specified URL, such as from a remote server. After the bootstrap image is loaded, the bootstrap image loads the specified system image file. See the appropriate hardware installation guide for details on setting the configuration register and secondary bootstrap filename.

Use this command when you have attempted to load a system image but have run out of memory even after compressing the system image. Secondary bootstrap images allows you to load a larger system image through a smaller secondary image.

### Examples

The following example shows how to load the system image file named sysimage-2 by using a secondary bootstrap image:

```
Router# configure terminal
Router(config)# boot bootstrap bootflash:sysimage-2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>Boots the router manually.</td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the system image that the router loads at startup.</td>
</tr>
</tbody>
</table>


**boot config**

To specify the device and filename of the configuration file from which the system configures itself during initialization (startup), use the `boot config` command in global configuration mode. To return to the default location for the configuration file, use the `no` form of this command.

**Platforms Other than Cisco 7600 Series Router**

```plaintext
boot config file-system-prefix:[directory/]filename [nvbypass]
no boot config
```

**Cisco 7600 Series Router**

```plaintext
boot config device:filename [nvbypass]
no boot config
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>file-system-prefix</code></td>
<td>File system, followed by a colon (for example, <code>nvram:</code>, <code>flash:</code>, <code>slot0:</code>, <code>usbflash 0 9</code> ;, or <code>usbtokent 0 9</code> ;). The default is <code>nvram:</code>.</td>
</tr>
<tr>
<td><code>directory</code></td>
<td>(Optional) File system directory where the configuration file is located, followed by a forward slash (/).</td>
</tr>
<tr>
<td><code>filename</code></td>
<td>Name of the configuration file.</td>
</tr>
<tr>
<td><code>device</code></td>
<td>Device identification, followed by a colon; see the “Usage Guidelines” section for a list of the valid values.</td>
</tr>
<tr>
<td><code>nvbypass</code></td>
<td>(Optional) Specifies that the distilled configuration is not written to nonvolatile random access memory (NVRAM).</td>
</tr>
</tbody>
</table>

**Command Default**

The default location for the configuration file is NVRAM (`nvram:`).

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was added for the Cisco 7600 Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the cisco 7600 Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>Support for Class B file system platforms and the following file system prefix options were added: <code>usbflash 0 9</code> ;and <code>usbtokent 0 9</code> ;.</td>
</tr>
</tbody>
</table>

This command is available only on Class A and Class B file system platforms.

You set the CONFIG_FILE environment variable in the current running memory when you use the `boot config` command. This variable specifies the configuration file used for initialization (startup). The configuration file must be an ASCII file located in either NVRAM or flash memory.

The valid values for the `device` argument and colon are as follows:
• For systems that are configured with a Supervisor Engine 2, the valid values are bootflash:, const_nvram:, flash:, nvram:, slot0:, sup-slot0:, and sup-bootflash:

• For systems that are configured with a Supervisor Engine 720, the valid values are disk0: and disk1:

The configuration file must be an ASCII file that is located in the specified file system.

The disk0: and disk1: keywords are for Class C file systems.

The bootflash:, slot0:, and sup-bootflash: keywords are for Class A file systems.

For Class A flash file systems, the CONFIG_FILE environment variable specifies the file system and filename of the configuration file to use for initialization (startup). You set the CONFIG_FILE environment variable in the current running memory when you use the boot config command. This variable specifies the configuration file used for initialization (startup).

When you use the boot config command, you affect only the running configuration. You must save the environment variable setting to your startup configuration to place the information under ROM monitor control and to have the environment variable function as expected. Use the copy system:running-config nvram:startup-config command to save the environment variable from your running configuration to your startup configuration.

The software displays an error message and does not update the CONFIG_FILE environment variable in the following situations:

• You specify nvram: as the file system, and it contains only a distilled version of the configuration. (A distilled configuration is one that does not contain access lists.)

• You specify a configuration file in the filename argument that does not exist or is not valid.

The router uses the NVRAM configuration during initialization when the CONFIG_FILE environment variable does not exist or when it is null (such as at first-time startup). If the software detects a problem with NVRAM or the configuration it contains, the device enters setup mode.

When you use the no form of this command, the router returns to using the default NVRAM configuration file as the startup configuration.

You can display the contents of the BOOT, BOOTLDR, and the CONFIG_FILE environment variables using the show bootvar command. This command displays the settings for these variables as they exist in the startup configuration and in the running configuration if a running configuration setting differs from a startup configuration setting.

When the boot config command is used, the distilled configuration is written into NVRAM and the system configuration is written into the file specified by the boot config command. If the distilled configuration exceeds the size of NVRAM, the system configuration gets truncated. Use the nvbypass keyword to prevent the system configuration from being truncated when the distilled configuration is larger than the size of NVRAM.

Examples

The following example shows how to set the configuration file that is located in internal flash memory to configure itself during initialization. The third line copies the specification to the startup configuration, ensuring that this specification will take effect upon the next reload.

Router(config)# boot config flash:router-config
Router(config)# end
Router# copy system:running-config nvram:startup-config

Cisco IOS Configuration Fundamentals Command Reference
The following example instructs a Cisco 7500 series router to use the configuration file named router-config located on the flash memory card inserted in the second Personal Computer Memory Card Industry Association (PCMCIA) slot of the Route Switch Processor (RSP) card during initialization. The third line copies the specification to the startup configuration, ensuring that this specification will take effect upon the next reload.

Router (config)# boot config slot1:router-config
Router (config)# end
Router# copy system:running-config nvram:startup-config

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy system:running-config nvram:startup-config</td>
<td>Saves the environment variable from the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>show bootvar</td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
</tr>
</tbody>
</table>

### boot host

To specify the host-specific configuration file to be used at the next system startup, use the `boot host` command in global configuration mode. To restore the host configuration filename to the default, use the `no` form of this command.

**boot host command**

```
boot host remote-url
no boot host remote-url
```

**Syntax Description**

- `remote-url` Location of the configuration file. Use the following syntax:
  - `ftp: //username[:password]@[location]/directory]/filename`
  - `rcp: //username[location]/directory]/filename`
  - `tftp: //location/directory]/filename`

**Command Default**

If you do not specify a `filename` using this command, the router uses its configured host name to request a configuration file from a remote server. To form the configuration filename, the router converts its name to all lowercase letters, removes all domain information, and appends `-config` or `-config`.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command instructs the system to “Boot using host-specific configuration file x,” where x is the filename specified in the remote-url argument. In other words, this command specifies the remote location and filename of the host-specific configuration file to be used at the next system startup, as well as the protocol to be used to obtain the file.

Before using the `boot host` command, use the `service config` global configuration command to enable the loading of the specified configuration file at reboot time. Without this command, the router ignores the `boot host` command and uses the configuration information in NVRAM. If the configuration information in NVRAM is invalid or missing, the `service config` command is enabled automatically.

The network server will attempt to load two configuration files from remote hosts. The first is the network configuration file containing commands that apply to all network servers on a network. Use the `boot network` command to identify the network configuration file. The second is the host configuration file containing commands that apply to one network server in particular. Use the `boot host` command to identify the host configuration file.

Note

Usually, the `service config` command is used in conjunction with the `boot host` or `boot network` command. You must enter the `service config` command to enable the router to automatically configure the system from the file specified by the `boot host` or `boot network` command. With IOS software versions 12.3(2)T, 12.3(1)B, and later, you no longer have to specify the `service config` command for the `boot host` or `boot network` command to be active. If you specify both the `no service config` command and the `boot host` command, the router attempts to find the specified host configuration file. The `service config` command can also be used without the `boot host` or `boot network` command. If you do not specify host or network configuration filenames, the router uses the default configuration files. The default network configuration file is `network-confg`. The default host configuration file is `host-confg`, where host is the hostname of the router. If the Cisco IOS software cannot resolve its hostname, the default host configuration file is `router-confg`.

Loading a Configuration File Using `rcp`

The `rcp` software requires that a client send the remote username on each `rcp` request to the network server. If the server has a directory structure (such as UNIX systems), the `rcp` implementation searches for the configuration files starting in the directory associated with the remote username.

When you load a configuration file from a server using `rcp`, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the file-URL, if a username is specified.
2. The username set by the `ip rcmd remote-username` command, if the command is configured.
3. The router host name.

Note

An account for the username must be defined on the destination server. If the network administrator of the destination server did not establish an account for the username, this command will not execute successfully.

Loading a Configuration File Using `FTP`

The `FTP` protocol requires a client to send a remote username and password on each `FTP` request to a server. The username and password must be associated with an account on the FTP server. If the server has a directory structure, the configuration file or image copied from the directory is associated with the username on the server. Refer to the documentation for your FTP server for more details.
When you load a configuration file from a server using FTP, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the `boot host` command, if a username is specified.
2. The username set by the `ip ftp username` command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the `boot host` command, if a password is specified.
2. The password set by the `ip ftp password` command, if the command is configured.
3. The router forms a password `username @routername .domain` . The variable `username` is the username associated with the current session, `routername` is the configured host name, and `domain` is the domain of the router.

### Examples

The following example sets the host filename to wilma-config at address 192.168.7.19:

```
Router(config)# boot host tftp://192.168.7.19/usr/local/tftpdir/wilma-config
Router(config)# service config
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>boot network</code></td>
<td>Specifies the remote location and filename of the network configuration file to be used at the next system boot (startup).</td>
</tr>
<tr>
<td><code>service config</code></td>
<td>Enables autoloading of configuration files from a network server.</td>
</tr>
</tbody>
</table>

### boot network

To change the default name of the network configuration file from which to load configuration commands, use the `boot network` command in global configuration mode. To restore the network configuration filename to the default, use the `no` form of this command.

```
boot network remote-url
no boot network remote-url
```

#### Syntax Description

- **remote-url**: Location of the configuration file. Use the following syntax:
  - `ftp: [[[username[: password]@]location]/ directory]/ filename]`
  - `rcp: [[[username @]location]/ directory]/ filename]`
  - `tftp: [[[location]/ directory]/ filename]`

#### Command Default

The default `filename` is `network-config`.
This command instructs the system to “Boot using network configuration file x ,” where x is the filename specified in the remote-url argument. This command specifies the remote location and filename of the network configuration file to be used at the next system startup, as well as the protocol to be used to obtain the file.

When booting from a network server, routers ignore routing information, static IP routes, and bridging information. As a result, intermediate routers are responsible for handling FTP, rcp, or TFTP requests. Before booting from a network server, verify that a server is available by using the ping command.

Use the service config command to enable the loading of the specified configuration file at reboot time. Without this command, the router ignores the boot network command and uses the configuration information in NVRAM. If the configuration information in NVRAM is invalid or missing, the service config command is enabled automatically.

The network server will attempt to load two configuration files from remote hosts. The first is the network configuration file containing commands that apply to all network servers on a network. Use the boot network command to identify the network configuration file. The second is the host configuration file containing commands that apply to one network server in particular. Use the boot host command to identify the host configuration file.

Note

Usually, the service config command is used in conjunction with the boot host or boot network command. You must enter the service config command to enable the router to automatically configure the system from the file specified by the boot host or boot network command. With IOS software versions 12.3(2)T, 12.3(1)B, and later, you no longer have to specify the service config command for the boot host or boot network command to be active. If you specify both the no service config command and the boot host command, the router attempts to find the specified host configuration file. The service config command can also be used without the boot host or boot network command. If you do not specify host or network configuration filenames, the router uses the default configuration files. The default network configuration file is network-confg. The default host configuration file is host-confg, where host is the hostname of the router. If the Cisco IOS software cannot resolve its hostname, the default host configuration file is router-confg.

Loading a Configuration File Using rcp

The rcp software requires that a client send the remote username on each rcp request to the network server. If the server has a directory structure (such as UNIX systems), the rcp implementation searches for the configuration files starting in the directory associated with the remote username.

When you load a configuration file from a server using rcp, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the file-URL, if a username is specified.
2. The username set by the ip rcmd remote-username command, if the command is configured.
3. The router host name.
An account for the username must be defined on the destination server. If the network administrator of the destination server did not establish an account for the username, this command will not execute successfully.

**Note**

Loading a Configuration File Using FTP

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. The username and password must be associated with an account on the FTP server. If the server has a directory structure, the configuration file or image copied from the directory associated with the username on the server. Refer to the documentation for your FTP server for more details.

When you load a configuration file from a server using FTP, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the `boot network` command, if a username is specified.
2. The username set by the `ip ftp username` command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the `boot network` command, if a password is specified.
2. The password set by the `ip ftp password` command, if the command is configured.
3. The router forms a password `username @routername .domain`. The variable `username` is the username associated with the current session, `routername` is the configured host name, and `domain` is the domain of the router.

**Examples**

The following example changes the network configuration filename to bridge_9.1 and uses the default broadcast address:

```
Router(config)# boot network tftp:bridge_9.1
Router(config)# service config
```

The following example changes the network configuration filename to bridge_9.1, specifies that rcp is to be used as the transport mechanism, and gives 172.16.1.111 as the IP address of the server on which the network configuration file resides:

```
Router(config)# service config
Router(config)# boot network rcp://172.16.1.111/bridge_9.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot host</td>
<td>Specifies the remote location and filename of the host-specific configuration file to be used at the next system boot (startup).</td>
</tr>
<tr>
<td>service config</td>
<td>Enables autoloading of configuration files from a remote host.</td>
</tr>
</tbody>
</table>
**boot system**

To specify the system image that the router loads at startup, use one of the following `boot system` command in global configuration mode. To remove the startup system image specification, use the `no` form of this command.

**Loading System Image from a URL or a TFTP File**

`boot system {file-url|filename}`

`no boot system {file-url|filename}`

**Booting from a System Image in Internal Flash**

`boot system flash [flash-fs:][partition-number:]filename`

`no boot system flash [flash-fs:][partition-number:] filename`

**Booting from a MOP Server**

`boot system mop filename [mac-address] [interface]`

`no boot system mop filename [mac-address] [interface]`

**Booting from ROM**

`boot system rom`

`no boot system rom`

**Booting a System Image from a Network, TFTP, or FTP Server**

`boot system {rcp|tftp|ftp} filename [ip-address]`

`no boot system {rcp|tftp|ftp} filename [ip-address]`

---

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>file-url</code></td>
<td>The URL of the system image to load at system startup.</td>
</tr>
<tr>
<td><code>filename</code></td>
<td>The TFTP filename of the system image to load at system startup.</td>
</tr>
<tr>
<td><code>flash</code></td>
<td>On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from internal flash memory. If you omit all arguments that follow this keyword, the system searches internal Flash for the first bootable image. On the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from the flash system specified by the <code>flash-fs</code> argument. On the Cisco 1600 series and Cisco 3600 series routers, if you omit all optional arguments, the router searches internal flash memory for the first bootable image. On the Cisco 7000 family routers, when you omit all arguments that follow this keyword, the system searches the Personal Computer Memory Card Industry Association (PCMCIA) slot 0 for the first bootable image.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **flash-fs**: | (Optional) Flash file system containing the system image to load at startup. The colon is required. Valid file systems are as follows:  
- **flash**: --Internal flash memory on the Cisco 1600 series and Cisco 3600 series routers. For the Cisco 1600 series and Cisco 3600 series routers, this file system is the default if you do not specify a file system. This is the only valid file system for the Cisco 1600 series.  
- **bootflash**: --Internal flash memory in the Cisco 7000 family.  
- **slot0**: --First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. For the Cisco 7000 family routers, this file system is the default if you do not specify a file system.  
- **slot1**: --Flash memory card in the second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. |
| **partition-number**: | (Optional) Number of the flash memory partition that contains the system image to boot, specified by the optional `filename` argument. If you do not specify a filename, the router loads the first valid file in the specified partition of flash memory. This argument is valid only on routers that can be partitioned. |
| **filename**: | (Optional when used with the `boot system flash` command) Name of the system image to load at startup. This argument is case sensitive. If you do not specify a value for the `filename` argument, the router loads the first valid file in the following:  
- The specified flash file system  
- The specified partition of flash memory  
- The default flash file system if you also omitted the `flash-fs` argument |
| **mop**: | Boots the router from a system image stored on a DECNET Maintenance Operations Protocol (MOP) server. Do not use this keyword with the Cisco 3600 series or Cisco 7000 family routers. |
| **mac-address**: | (Optional) MAC address of the MOP server containing the specified system image file. If you do not include the MAC address argument, the router sends a broadcast message to all MOP boot servers. The first MOP server to indicate that it has the specified file is the server from which the router gets the boot image. |
| **interface**: | (Optional) Interface the router uses to send out MOP requests to the MOP server. The interface options are `async`, `dialer`, `ethernet`, `serial`, and `tunnel`. If you do not specify the `interface` argument, the router sends a request out on all interfaces that have MOP enabled. The interface that receives the first response is the interface the router uses to load the software. |
| **rom**: | Boots the router from ROM. Do not use this keyword with the Cisco 3600 series or the Cisco 7000 family routers. |
| **rcp**: | Boots the router from a system image stored on a network server using rcp. |
### Command Default

If you configure the router to boot from a network server but do not specify a system image file with the `boot system` command, the router uses the configuration register settings to determine the default system image filename. The router forms the default boot filename by starting with the word `cisco` and then appending the octal equivalent of the boot field number in the configuration register, followed by a hyphen (-) and the processor type name (cisconn-cpu). Refer to the appropriate hardware installation guide for details on the configuration register and default filename. See also the `config-register` or `confreg` command.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For this command to work, the `config-register` command must be set properly.

Create a comma-delimited list of several `boot system` commands to provide a fail-safe method for booting your router. The router stores and executes the `boot system` commands in the order in which you enter them in the configuration file. If you enter multiple boot commands of the same type—for example, if you enter two commands that instruct the router to boot from different network servers—the router tries them in the order in which they appear in the configuration file. If a `boot system` command entry in the list specifies an invalid device, the router omits that entry. Use the `boot system rom` command to specify use of the ROM system image as a backup to other `boot system` commands in the configuration.

#### Note

After a list of several images are specified with the `boot system` command, running the command again results in the list being appended, not removed.

For some platforms, the boot image must be loaded before the system image is loaded. However, on many platforms, the boot image is loaded only if the router is booting from a network server or if the flash file system is not specified. If the file system is specified, the router will boot faster because it need not load the boot image first.

This section contains the following topics:

- Changing the List of Boot System Commands

### boot system

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tftp</td>
<td>Boots the router from a system image stored on a TFTP server.</td>
</tr>
<tr>
<td>ftp</td>
<td>Boots the router from a system image stored on an FTP server.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(Optional) IP address of the server containing the system image file. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.</td>
</tr>
</tbody>
</table>
• Booting Compressed Images
• Understanding rcp
• Understanding TFTP
• Understanding FTP
• Stopping Booting and Entering ROM Monitor Mode
• Cisco 1600 Series, Cisco 3600 Series, Cisco 7000 Family, and Cisco 7600 Series Router Notes

Changing the List of Boot System Commands

To remove a single entry from the bootable image list, use the no form of the command with an argument. For example, to remove the entry that specifies a bootable image on a flash memory card inserted in the second slot, use the no boot system flash slot1: filename] command. All other entries in the list remain.

To eliminate all entries in the bootable image list, use the no boot system command. At this point, you can redefine the list of bootable images using the previous boot system commands. Remember to save your changes to your startup configuration by issuing the copy system:running-config nvram:startup-config command.

Each time you write a new software image to flash memory, you must delete the existing filename in the configuration file with the no boot system flash filename command. Then add a new line in the configuration file with the boot system flash filename command.

Note

If you want to rearrange the order of the entries in the configuration file, you must first issue the no boot system command and then redefine the list.

Booting Compressed Images

You can boot the router from a compressed image on a network server. When a network server boots software, both the image being booted and the running image must be able to fit into memory. Use compressed images to ensure that enough memory is available to boot the router. You can compress a software image on any UNIX platform using the compress command. Refer to your UNIX platform’s documentation for the exact usage of the compress command. (You can also uncompress data with the UNIX uncompress command.)

Understanding rcp

The rcp requires that a client send the remote username in an rcp request to a server. When the router executes the boot system rcp command, the Cisco IOS software sends the hostname as both the remote and local usernames by default. Before the rcp can execute properly, an account must be defined on the network server for the remote username configured on the router.

If the server has a directory structure, the rcp software searches for the system image to boot from the remote server relative to the directory of the remote username.

By default, the router software sends the hostname as the remote username. You can override the default remote username by using the ip remd remote-username command. For example, if the system image resides in the home directory of a user on the server, you can specify that user’s name as the remote username.

Understanding TFTP

You need a TFTP server running to retrieve the router image from the host.

Understanding FTP
You need an FTP server running to retrieve the router image from the host. You also need an account on the server or anonymous file access to the server.

**Stopping Booting and Entering ROM Monitor Mode**

During the first 60 seconds of startup, you can force the router to stop booting by pressing the Break key. The router will enter ROM monitor mode, where you can change the configuration register value or boot the router manually.

**Cisco 1600 Series, Cisco 3600 Series, Cisco 7000 Family, and Cisco 7600 Series Router Notes**

For the Cisco 3600 series and Cisco 7000 family, the `boot system` command modifies the BOOT variable in the running configuration. The BOOT variable specifies a list of bootable images on various devices.

---

**Note**

When you use the `boot system` command on the Cisco 1600 series, Cisco 3600 series, Cisco 7000 family, and Cisco 7600 series, you affect only the running configuration. You must save the BOOT variable settings to your startup configuration to place the information under ROM monitor control and to have the variable function as expected. Use the `copy system:running-config nvram:startup-config` privileged EXEC command to save the variable from your running configuration to your startup configuration.

To display the contents of the BOOT variable, use the `show bootvar` EXEC command.

---

**Examples**

The following example illustrates a configuration that specifies two possible internetwork locations for a system image, with the ROM software being used as a backup:

```
Router(config)# boot system tftp://192.168.7.24/cs3-rx.90-1
Router(config)# boot system tftp://192.168.7.19/cs3-rx.83-2
Router(config)# boot system rom
```

The following example boots the system boot relocatable image file named igs-bpx-l from partition 2 of the flash device:

```
Router(config)# boot system flash:2:igs-bpx-l
```

The following example instructs the router to boot from an image located on the flash memory card inserted in slot 0:

```
Router(config)# boot system slot0:new-config
```

The following example specifies the file named new-ios-image as the system image for a Cisco 3600 series router to load at startup. This file is located in the fourth partition of the flash memory card in slot 0:

```
Router(config)# boot system slot0:4:dirt/images/new-ios-image
```

This example boots from the image file named c1600-y-l in partition 2 of flash memory of a Cisco 1600 series router:

```
Router(config)# boot system flash:2:c1600-y-l
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>Boots the router manually.</td>
</tr>
<tr>
<td>config-register</td>
<td>Changes the configuration register settings.</td>
</tr>
<tr>
<td>confreg</td>
<td>Changes the configuration register settings while in ROM monitor mode.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>copy system:running-config nvram:startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>ip rcmd remote username</td>
<td>Configures the remote username to be used when requesting a remote copy using rcp.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting.</td>
</tr>
</tbody>
</table>

---

**boot-end-marker**

The **boot-start-marker** and **boot-end-marker** flags, which can be seen in Cisco IOS software configuration files, are not CLI commands. These markers are written to configuration files automatically to flag the beginning and end of the boot commands (boot statements). By flagging boot statements, these markers allow the router to more reliably load Cisco IOS images during bootup.

A boot statement is one or more lines in a configuration file that tells the router which software image to load after a powercycling (reboot). The boot-start-marker and boot-end-marker flags will appear around any boot commands, including:

- boot bootstrap
- boot config
- boot host
- boot network
- boot system

Note, however, that these markers will always appear in the output of the **show running-config** or **more system:running-config** commands, regardless of whether any actual boot commands have been entered. This means that no boot commands will appear between the markers if no boot commands have been entered, or if all boot commands have been removed from the configuration, as shown in the “Examples” section.

The **boot-start-marker** and **boot-end-marker** flags cannot be removed or modified using the CLI. These markers are written to the startup configuration file whenever a **copy running-config startup-config** command is issued.

These flags were also introduced to circumvent errors in the configuration file, such as a leading space before a boot command (such as those sometimes introduced by manually edited configuration files), or the use of text strings that include the word “boot” in banners or other user-specified text.
If the “boot start-marker” flag is not found in the configuration file, the system will use the traditional method to identify the boot commands. However, if you are manually creating configuration files, or copying from older Cisco IOS software releases, the addition of these markers is recommended.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(3), 12.3(4)T, 12.0(26)S, 12.0(27)SV, 12.3(3)B,</td>
<td>The <strong>boot-start-marker</strong> and <strong>boot-end-marker</strong> flags were introduced.</td>
</tr>
</tbody>
</table>

### Examples

In the following example, a **boot** command is entered, and the boot-start-marker and boot-end-marker flags are shown in the context of the startup configuration file:

```plaintext
Router# configure terminal
Enter configuration commands, one per line. End with the end command.
Router(config)# boot system slot0:
Router(config)# end
Router# copy running-config startup-config
Router# show startup-config
Using 1398 out of 129016 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname C3660-2
!
boot-start-marker
boot system slot0:
boot-end-marker
!
logging count
.
.
In the following example, the boot-start-marker and boot-end-marker flags appear in the configuration file even though no **boot** commands have been entered:

```plaintext
Router# show running-configuration
Current configuration :3055 bytes
!
! No configuration change since last restart
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
```
### boot-start-marker

The `boot-start-marker` and `boot-end-marker` flags, which can be seen in Cisco IOS software configuration files, are not CLI commands. These markers are written to configuration files automatically to flag the beginning and end of the boot commands (boot statements). By flagging boot statements, these markers allow the router to more reliably load Cisco IOS images during bootup.

A boot statement is one or more lines in a configuration file that tells the router which software image to load after a power cycling (reboot). The boot-start-marker and boot-end-marker flags will appear around any boot commands, including:

- `boot bootstrap`
- `boot config`
- `boot host`
- `boot network`
- `boot system`

Note, however, that these markers will always appear in the output of the `show running-config` or `more system:running-config` commands, regardless of whether any actual boot commands have been entered. This means that no boot commands will appear between the markers if no boot commands have been entered, or if all boot commands have been removed from the configuration, as shown in the “Examples” section.

The `boot-start-marker` and `boot-end-marker` flags cannot be removed or modified using the CLI. These markers are written to the startup configuration file whenever a `copy running-config startup-config` command is issued.

These flags were also introduced to circumvent errors in the configuration file, such as a leading space before a boot command (such as those sometimes introduced by manually edited configuration files), or the use of text strings that include the word “boot” in banners or other user-specified text.

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>boot bootstrap</code></td>
<td>Specifies the filename and location of a secondary bootstrap image (to be used if a valid software image cannot be loaded).</td>
</tr>
<tr>
<td><code>boot config</code></td>
<td>Specifies the device and filename of the configuration file from which the router boots during startup (for Class A filesystems).</td>
</tr>
<tr>
<td><code>boot host</code></td>
<td>Specifies a remote host location for the host-specific (router-specific) configuration file to be used at the next system startup.</td>
</tr>
<tr>
<td><code>boot network</code></td>
<td>Specifies a remote location for the network (network-wide) configuration file to be used at the next system startup.</td>
</tr>
<tr>
<td><code>boot system</code></td>
<td>Specifies the system software image that the router loads at startup.</td>
</tr>
</tbody>
</table>
If the “boot start-marker” flag is not found in the configuration file, the system will use the traditional method to identify the boot commands. However, if you are manually creating configuration files, or copying from older Cisco IOS software releases, the addition of these markers is recommended.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(3), 12.3(4)T, 12.0(26)S, 12.0(27)SV, 12.3(3)B</td>
<td>The <code>boot-start-marker</code> and <code>boot-end-marker</code> flags were introduced.</td>
</tr>
</tbody>
</table>

### Examples

In the following example, a `boot` command is entered, and the boot-start-marker and boot-end-marker flags are shown in the context of the startup configuration file:

Router# configure terminal

Enter configuration commands, one per line. End with the `end` command.

Router(config)# boot system slot0:

Router(config)# end

Router# copy running-config startup-config

Router# show startup-config

Using 1398 out of 129016 bytes

version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

! hostname C3660-2

boot-start-marker
boot system slot0:
boot-end-marker

! logging count
.
.
.

In the following example, the boot-start-marker and boot-end-marker flags appear in the configuration file even though no `boot` commands have been entered:

Router# show running-configuration

Current configuration :3055 bytes

! No configuration change since last restart

! version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

! hostname Router

! boot-start-marker
boot-end-marker

!
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot bootstrap</td>
<td>Specifies the filename and location of a secondary bootstrap image (to be used if a valid software image cannot be loaded).</td>
</tr>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the router boots during startup (for Class A fileytems).</td>
</tr>
<tr>
<td>boot host</td>
<td>Specifies a remote host location for the host-specific (router-specific) configuration file to be used at the next system startup.</td>
</tr>
<tr>
<td>boot network</td>
<td>Specifies a remote location for the network (network-wide) configuration file to be used at the next system startup.</td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the system software image that the router loads at startup.</td>
</tr>
</tbody>
</table>
C commands

- C commands, on page 62
C commands

cd

To change the default directory or file system, use the cd command in user EXEC or privileged EXEC mode.

```
cd [filesystem:][directory]
```

**Syntax Description**

| filesystem | (Optional) The URL or alias of the directory or file systems followed by a colon. |
| directory  | (Optional) Name of the directory. |

**Command Default**

The initial default file system is `flash:`. For platforms that do not have a physical device named `flash:`, the keyword `flash:` is aliased to the default Flash device.

For the Supervisor Engine, the initial default file system is `disk0`:

If you do not specify a directory on a file system, the default is the root directory on that file system.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)SX, and support was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support was added for the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The valid values for `filesystem` are as follows:

- For systems that are configured with a Supervisor Engine 2, valid values are `bootflash:`, `const_nvram:`, `disk0:`, `flash:`, `nvram:`, `slot0:`, `sup-slot0:`, and `sup-bootflash:`
- For systems that are configured with a Supervisor Engine 720, valid values are `disk0:` and `disk1:`

For all EXEC commands that have an optional `filesystem` argument, the system uses the file system specified by the `cd` command when you omit the optional `filesystem` argument. For example, the `dir` command, which displays a list of files on a file system, contains an optional `filesystem` argument. When you omit this argument, the system lists the files on the file system specified by the `cd` command.

If you do not specify a directory on a file system, the default is the root directory on that file system.

**Examples**

In the following example, the `cd` command is used to set the default file system to the Flash memory card inserted in slot 0:
Router# pwd
bootflash:/
Router# cd slot0:
Router#
pwd
slot0:/

Cisco 7600 Series

This example sets the default file system to the Flash PC card that is inserted in disk 0:

Router# cd disk0:
Router#
pwd
disk0: /

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Deletes a file on a Flash memory device.</td>
</tr>
<tr>
<td></td>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td></td>
<td>mkdir disk0:</td>
<td>Creates a new directory in a Flash file system.</td>
</tr>
<tr>
<td></td>
<td>pwd</td>
<td>Displays the current setting of the cd command.</td>
</tr>
<tr>
<td></td>
<td>show file systems</td>
<td>Lists available file systems and their alias prefix names.</td>
</tr>
<tr>
<td></td>
<td>undelete</td>
<td>Recovers a file marked “deleted” on a Class A or Class B Flash file system.</td>
</tr>
</tbody>
</table>

**clear archive log config**

To purge the configuration logging database entries, use the `clear archive log config` command in privileged EXEC mode.

```
clear archive log config [{force|persistent}] 
```

**Syntax Description**

<table>
<thead>
<tr>
<th>force</th>
<th>(Optional) Eliminates the confirm step before the contents of the archive log are cleared.</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent</td>
<td>(Optional) Purges the configuration logging persistent-command database entries.</td>
</tr>
</tbody>
</table>

**Command Default**

If this command is not used, the database entries accumulate in the archive log.

**Command Modes**

Privileged EXEC (#)
clear catalyst6000 traffic-meter

To clear the traffic meter counters, use the clear catalyst6000 traffic-meter command in privileged EXEC mode.

clear catalyst6000 traffic-meter

Syntax Description
This command has no arguments or keywords.

Command Default
This command has no default settings.

Command Modes
Privileged EXEC

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17a)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples
This example shows how to clear the traffic meter counters:

Router# clear catalyst6000 traffic-meter
Router#
clear configuration lock

To clear the lock on the running configuration file, use the `clear configuration lock` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(25)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was enhanced to allow the exclusive configuration lock to be cleared during erratic or abnormal behavior.</td>
</tr>
<tr>
<td>12.0(31)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(31)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `clear configuration lock` command when the running configuration file is not locked by the `configure replace` command:

Router# clear configuration lock
Parser Config not locked.

The following is sample output from the `clear configuration lock` command when the running configuration file is locked by the `configure replace` command:

Router# clear configuration lock
Process <3> is holding the EXCLUSIVE lock!
Do you want to clear the lock?[confirm] y

The following example shows how to use the `clear configuration lock` command to display the owner or process ID of the lock and prompt the user for confirmation:

Router# clear configuration lock
Process <46> is holding the EXCLUSIVE lock.
Do you want to clear the lock?[confirm] y

After the lock is cleared, a message will be sent to the terminal if the owner of the lock is a TTY user:

Router(config)# The configuration lock was cleared by user <steve> from terminal <5>
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration mode exclusive</td>
<td>Enables single-user (exclusive) access functionality for the Cisco IOS CLI.</td>
</tr>
<tr>
<td>debug configuration lock</td>
<td>Enables debugging of the Cisco IOS configuration lock.</td>
</tr>
<tr>
<td>show configuration lock</td>
<td>Displays information about the lock status of the running configuration file during a configuration replace operation.</td>
</tr>
</tbody>
</table>

**clear diagnostic event-log**

To clear the diagnostic event logs for a specific module or event type, use the `clear diagnostic event-log` command in privileged EXEC mode.

`clear diagnostic event-log {event-type {error|info|warning}|module {num|slot subslot|all}}`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event-type error</td>
<td>Specifies clearing error events.</td>
</tr>
<tr>
<td>event-type info</td>
<td>Specifies clearing informative events.</td>
</tr>
<tr>
<td>event-type warning</td>
<td>Specifies clearing warning events.</td>
</tr>
<tr>
<td>module num</td>
<td>Specifies clearing events for a specific module.</td>
</tr>
<tr>
<td>module slot subslot</td>
<td>Specifies clearing all linecards.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear diagnostic event-log` command clears all the events for all the modules.

The `clear diagnostic event-log module num` command clears events only for a specific module.

The `clear diagnostic event-log event-type` command clears only specific event types such as error, informative, or warning events.

**Examples**

This example shows how to clear error event logs:

```
Router# clear diagnostic event-log event-type error
```

This example shows how to clear event logs on module 3:

```
Router# clear diagnostic event-log module 3
```

This example shows how to clear error event logs on all the modules:
clear diagnostic event-log module all

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic events</td>
<td>Displays the diagnostic event log</td>
</tr>
</tbody>
</table>

clear ip http client cache

To remove information from the HTTP client cache, use the `clear ip http client cache` command in privileged EXEC mode.

`clear ip http client cache {all|session session-name|url complete-url}`

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cache all</code></td>
<td>Removes all HTTP client cache entries.</td>
</tr>
<tr>
<td><code>cache session</code></td>
<td>Removes HTTP client cache entries of the HTTP client application session specified by the <code>session-name</code> argument.</td>
</tr>
<tr>
<td><code>cache url</code></td>
<td>Removes the HTTP client cache entry whose location is specified by the <code>complete-url</code> argument, a Cisco IOS File System (IFS) Uniform Resource Locator (URL), and that consists of HTML files used by an HTTP server.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to clear entries from the HTTP client cache pool: all the entries, all the entries owned by a specific session, or only the entry associated with a specific request from an HTTP server.

Examples

The following example clears all entries in the HTTP client cache:

Router# clear ip http client cache all

The following example removes HTTP client cache entries that belong to the HTTP Client File System (CFS) application:

Router# clear ip http client cache session HTTP CFS

The following example removes HTTP client cache entries at the location http://myrouter.cisco.com/flash:/

Router# clear ip http client cache url http://myrouter.cisco.com/flash:/
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip http path</td>
<td>Specifies the base path used to locate files for use by the HTTP server.</td>
</tr>
<tr>
<td>show ip http client</td>
<td>Displays a report about the HTTP client.</td>
</tr>
</tbody>
</table>

**clear logging**

To clear messages from the logging buffer, use the `clear logging` command in privileged EXEC mode.

```
clear logging [persistent [url filesystem/directory]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent</td>
<td>(Optional) Deletes persistent logging files.</td>
</tr>
<tr>
<td>url</td>
<td>(Optional) Specifies the URL for storing logging messages.</td>
</tr>
<tr>
<td>filesystem:</td>
<td>The file system followed by a colon.</td>
</tr>
<tr>
<td>/directory</td>
<td>The directory on the filesystem. The slash is required.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was modified. The <code>persistent</code> and <code>url</code> keywords, and the <code>filesystem/directory</code> arguments were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear logging persistent` command is used to remove stored audit records. This action can be performed by the audit administrator only. The `clear logging persistent` command clears only log files stored in the directory but does not remove the directory itself. If no log URL is not specified for logging, this command clears files from the location as specified in the `logging persistent` command.

**Examples**

In the following example, the logging buffer is cleared:

```
Router# clear logging
Clear logging buffer [confirm]
```

The following example shows how to clear persistent logging files:

```
Router# clear logging persistent
Delete persistent logging files from bootflash:/audit_log ? [confirm]
Router# dir bootflash:/audit_log
Directory of bootflash:/audit_log/
No files in directory
```

The following example shows how to clear persistent logging files from a specific directory:
clear logging system

To clear event records stored in the System Event Archive (SEA) log file sea_log.dat, use the **clear logging system** command in user EXEC mode.

`clear logging system [disk name]`

**Syntax Description**

| disk name  | (Optional) Stores the system event log in the specified disk. |

**Command Default**

This command has no default settings.

**Command Modes**

User EXEC (>)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>This command was introduced for the Cisco uBR10012 router in the Cisco IOS Software Release 12.2(33)SCC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SEA is supported on switches that have a Supervisor Engine 32 or Supervisor Engine 720 with a compact flash adapter and a Compact Flash card (WS-CF-UPG= for Supervisor Engine 720).

**Cisco Universal Broadband Router 10012**

The SEA feature is used to address debug trace and system console constraints. SEA is a logging feature that allows the modules in the system to report major and critical events to the route processor (RP). The events occurring on the line card or jacket card are also sent to the RP using Inter-Process Communication (IPC) capability. Use the **clear logging system** command to clear the event records stored in the SEA log file.

**Note**

To store the system event logs, the SEA requires either the PCMCIA ATA disk or Compact Flash Disk in compact flash adapter for PRE2.
Examples

This example shows how to clear the SEA:

Router# clear logging system
Clear logging system operation will take a while.
Do you want to continue? [no]: yes
Router#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy logging system</td>
<td>Copies the archived system events to another location.</td>
</tr>
<tr>
<td>logging system</td>
<td>Enables or disables the SEA logging system.</td>
</tr>
<tr>
<td>show logging system</td>
<td>Displays the SEA logging system disk.</td>
</tr>
</tbody>
</table>

clear logging xml

To clear the contents of the XML system message logging (syslog) buffer, use the clear logging xml command in User EXEC or Privileged EXEC mode.

clear logging xml

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command clears the contents of the XML-formatted logging buffer, but does not clear the contents of the standard logging buffer. The system will prompt you to confirm the action before clearing the buffer.

Examples

In the following example, the XML-specific buffer is cleared:

Router# clear logging xml
Clear XML logging buffer [confirm]? y

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging buffered xml</td>
<td>Enables system message logging (syslog) to the XML-specific buffer in XML format.</td>
</tr>
</tbody>
</table>
clear memory low-water-mark

To clear the low-water-mark memory, use the `clear memory low-water-mark` command in privileged EXEC mode.

**clear memory low-water-mark**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced into a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command clears all processor threshold values and the input/output memory threshold values, if any.

**Examples**

The following example shows how to clear the low-water-mark memory:

```
Router# clear memory low-water-mark
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory free low-watermark</td>
<td>Configures a router to issue system logging message notifications when available memory falls below a specified threshold.</td>
</tr>
</tbody>
</table>

clear mls statistics

To reset the Multilayer Switching (MLS) statistics counters, use the `clear mls statistics` command in privileged EXEC mode.

**clear mls statistics [module num]**
clear parser cache

To clear the parse cache entries and hit/miss statistics stored for the Parser Cache feature, use the `clear parser cache` command in privileged EXEC mode.

**clear parser cache**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC
clear parser statistics

This command was introduced in Cisco IOS Release 15.0S.

Usage Guidelines

The clear parser statistics command will free the system memory used for recording parser performance statistics stored for the output of the show parser statistics EXEC command.

Examples

The following example shows the clearing of the parser cache:

Router# show parser statistics
Last configuration file parsed: Number of Commands: 1484, Time: 820 ms
Parser cache: enabled, 1460 hits, 26 misses
Router# clear parser cache
Router# show parser statistics
Last configuration file parsed: Number of Commands: 1484, Time: 820 ms
Parser cache: enabled, 0 hits, 1 misses

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parser cache</td>
<td>Enables or disables the Parser Cache feature.</td>
</tr>
<tr>
<td>show parser statistics</td>
<td>Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.</td>
</tr>
</tbody>
</table>

clear parser statistics

To clear the parser performance statistics, use the clear parser statistics command in privileged EXEC mode.

clear parser statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release  Modification
15.0S       This command was introduced.

Usage Guidelines

The clear parser statistics command will free the system memory used for recording parser performance statistics stored for the output of the show parser statistics EXEC command.
Examples

The following example shows the clearing parser statistics:

Router# show parser statistics
Last configuration file parsed: Number of Commands: 1, Time: 31 ms

Parser cache: enabled, 129 hits, 46 misses
Active startup time: 0
Standby startup time: 186
Copy to running-config time:0
Bulksync time:0

Top 10 slowest command:

<table>
<thead>
<tr>
<th>Function</th>
<th>Time (ms)</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xE71F90</td>
<td>7</td>
<td>shutdown</td>
</tr>
<tr>
<td>0x1235280</td>
<td>11</td>
<td>no ip address</td>
</tr>
<tr>
<td>0x1235280</td>
<td>11</td>
<td>no ip address</td>
</tr>
<tr>
<td>0x1235280</td>
<td>11</td>
<td>no ip address</td>
</tr>
<tr>
<td>0x1235280</td>
<td>12</td>
<td>no ip address</td>
</tr>
<tr>
<td>0x1235280</td>
<td>12</td>
<td>no ip address</td>
</tr>
<tr>
<td>0x1235280</td>
<td>12</td>
<td>no ip address</td>
</tr>
<tr>
<td>0x1235280</td>
<td>12</td>
<td>no ip address</td>
</tr>
<tr>
<td>0xD6C940</td>
<td>6170</td>
<td>show run</td>
</tr>
</tbody>
</table>

Parser last bootup cache hits:
  - Bootup hits:125
  - Bootup misses:43
  - Bootup clear parser cache:0

Router# clear parser statistics
func=E01730, duration=0 cmd= clear parser statistics

Router# show parser statistics
Last configuration file parsed: Number of Commands: 0, Time: 0 ms

Parser cache: enabled, 130 hits, 47 misses
Active startup time: 0
Standby startup time: 0
Copy to running-config time:0
Bulksync time:0

Top 10 slowest command:

<table>
<thead>
<tr>
<th>Function</th>
<th>Time (ms)</th>
<th>Command</th>
</tr>
</thead>
</table>

Parser last bootup cache hits:
  - Bootup hits:0
  - Bootup misses:0
  - Bootup clear parser cache:0

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parser cache</td>
<td>Enables or disables the Parser Cache feature.</td>
</tr>
<tr>
<td>show parser statistics</td>
<td>Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.</td>
</tr>
</tbody>
</table>
clear platform netint

To clear the interrupt-throttling counters for the platform, use the clear platform netint command in privileged EXEC mode.

clear platform netint

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17b)SXA</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release</td>
</tr>
<tr>
<td></td>
<td>12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to clear the interrupt-throttling counters for the platform:

Router# clear platform netint
Router#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform netint</td>
<td>Displays the platform network-interrupt information.</td>
</tr>
</tbody>
</table>

clear processes interrupt mask

To clear interrupt mask details for all processes in the interrupt mask buffer, use the clear processes interrupt mask detail command in privileged EXEC mode.

clear processes interrupt mask detail

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced as part of the Process Interrupt Mask Profiler Enhancement feature.</td>
</tr>
</tbody>
</table>
Usage Guidelines

See the documentation of the scheduler interrupt mask commands (listed in the Related Commands table) for further details on process interrupt mask profiling.

Examples

The following example demonstrates how to clear interrupt mask statistics from system memory for all processes:

```
Router# clear processes interrupt mask detail
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>scheduler interrupt mask profile</td>
<td>Starts interrupt mask profiling for all processes running on the system</td>
</tr>
<tr>
<td></td>
<td>scheduler interrupt mask size</td>
<td>Configures the maximum number of entries that can exist in the interrupt mask buffer.</td>
</tr>
<tr>
<td></td>
<td>scheduler interrupt mask time</td>
<td>Configures the maximum time that a process can run with interrupts masked.</td>
</tr>
<tr>
<td></td>
<td>show process interrupt mask buffer</td>
<td>Displays the information stored in the interrupt mask buffer.</td>
</tr>
<tr>
<td></td>
<td>show processes interrupt mask detail</td>
<td>Displays interrupt masked details for the specified processes or all processes in the system.</td>
</tr>
</tbody>
</table>

**clear scp accounting**

To clear the Switch-Module Configuration Protocol (SCP) accounting information, use the `clear scp accounting` command in privileged EXEC mode.

```
clear scp accounting
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced into a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the SCP accounting information:

```
Router# clear scp accounting
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show scp</td>
<td>Displays SCP information.</td>
</tr>
</tbody>
</table>
clear tcp

To clear a TCP connection, use the `clear tcp` command in privileged EXEC mode.

```
clear tcp {line line-number|local hostname port remote hostname port|tcb address}
```

**Syntax Description**

- **line line-number**: Line number of the TCP connection to clear.
- **local hostname port remote hostname port**: Host name of the local router and port and host name of the remote router and port of the TCP connection to clear.
- **tcb address**: Transmission Control Block (TCB) address of the TCP connection to clear. The TCB address is an internal identifier for the endpoint.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear tcp` command is particularly useful for clearing hung TCP connections.

The `clear tcp line line-number` command terminates the TCP connection on the specified tty line. Additionally, all TCP sessions initiated from that tty line are terminated.

The `clear tcp local hostname port remote hostname port` command terminates the specific TCP connection identified by the host name and port pair of the local and remote router.

The `clear tcp tcb address` command terminates the specific TCP connection identified by the TCB address.

**Examples**

The following example clears a TCP connection using its tty line number. The `show tcp` command displays the line number (tty2) that is used in the `clear tcp` command.

```
Router# show tcp

tty2, virtual tty from host router20.cisco.com
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 171.69.233.7, Local port: 23
Foreign host: 171.69.61.75, Foreign port: 1058

Enqueued packets for retransmit: 0, input: 0, saved: 0

Event Timers (current time is 0x36144):

<table>
<thead>
<tr>
<th>Timer</th>
<th>Starts</th>
<th>Wakeups</th>
<th>Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrans</td>
<td>4</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>TimeWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>AckHold</td>
<td>7</td>
<td>4</td>
<td>0x0</td>
</tr>
<tr>
<td>SendWnd</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>GiveUp</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>PmtuAger</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
</tbody>
</table>

iss: 4151109680 snduna: 4151109752 sndnxt: 4151109752 sndwnd: 24576
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tcp</td>
<td>Displays the status of TCP connections.</td>
</tr>
<tr>
<td>show tcp brief</td>
<td>Displays a concise description of TCP connection endpoints.</td>
</tr>
</tbody>
</table>

**clear vlan counters**

To clear the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs, use the **clear vlan counters** command in privileged EXEC mode.

**clear vlan [vlan-id] counters**

**Syntax Description**

- **vlan-id** (Optional) The ID of a specific VLAN. Range: 1 to 4094.

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you do not specify a `vlan-id`; the software-cached counter values for all existing VLANs are cleared.

Examples

This example shows how to clear the software-cached counter values for a specific VLAN:

```plaintext
Router# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm]y
Router#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vlan counters</code></td>
<td>Displays the software-cached counter values.</td>
</tr>
</tbody>
</table>

**clock**

To configure the port clocking mode for the 1000BASE-T transceivers, use the `clock` command in interface configuration mode. To return to the default settings, use the `no` form of this command.

```
clock {auto|active [prefer]|passive [prefer]}
no clock
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enables the automatic-clock configuration.</td>
</tr>
<tr>
<td>active</td>
<td>Enables the active operation.</td>
</tr>
<tr>
<td>prefer</td>
<td>(Optional) Negotiates the specified mode with the far end of the link.</td>
</tr>
<tr>
<td>passive</td>
<td>Enables the passive operation.</td>
</tr>
</tbody>
</table>

Command Default

`auto`

Command Modes

Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17a)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is supported on the 1000BASE-T transceivers only.
If the clock mode of the near end of a link does not match the clock mode of the far end, the line protocol
does not come up.

The active and passive clock status is determined during the auto negotiation process before the transmission
link is established.

The clock command supports the following configurations:

- **auto** -- Auto negotiates with the far end of the link but preference is given to the active-clock switch.
- **active** -- Uses a local clock to determine transmitter-operation timing.
- **passive** -- Recovers the clock from the received signal and uses the recovered clock to determine
  transmitter-operation timing.
- **active prefer** -- Auto negotiates with the far end of the link but preference is given to the active-clock
  switch.
- **passive prefer** -- Auto negotiates with the far end of the link but preference is given to the passive-clock
  switch.

Enter the show running-config interface command to display the current clock mode.
Enter the show interfaces command to display the clock mode that is negotiated by the firmware.

### Examples

This example shows how to enable the active-clock operation:

```
Router(config-if)# clock active
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays traffic that is seen by a specific interface.</td>
</tr>
<tr>
<td>show running-config interface</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>

### clock initialize nvram

To restart the system clock from the last known system clock value, use the clock initialize nvram command
in global configuration mode. To disable the restart of the system clock from the last known system clock
value, use the no form of this command.

```
clock initialize nvram
no clock initialize nvram
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, the system clock is set to restart from the last known system clock value for platforms that have
no hardware calendar.

**Command Modes**

Global configuration (config)
Usage Guidelines

For platforms that have hardware calendars, the `clock initialize nvram` command is not available. When the `no` form of the command is configured, the system clock gets initialized to default standard values. The default values can be either 1MAR1993 or 1MAR2002.

Examples

The following example shows how to set the system clock to restart from the last known system clock value:

```
Router(config)# clock initialize nvram
```

**config-register**

To change the configuration register settings, use the `config-register` command in global configuration mode.

```
config-register  value
```

**Syntax Description**

```
value  Hexadecimal or decimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF (0 to 65535 in decimal).
```

**Command Default**

Refer to the documentation for your platform for the default configuration register value. For many newer platforms, the default is 0x2102, which causes the router to boot from Flash memory and the Break key to be ignored.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command applies only to platforms that use a software configuration register.

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.

To change the boot field value and leave all other bits set to their default values, follow these guidelines:

* If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the `boot` command.
• If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.

• If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.

For more information about the configuration register bit settings and default filenames, refer to the appropriate router hardware installation guide.

**Note**

In a virtual switch application, if you have configured your config-register with a value that would skip file parsing during the bootup process, your change to either a standalone or virtual switch will not take place until you reconfigure your config-register. The config-register must be allowed to parse files in order to ensure the conversion from either a standalone or virtual switch.

**Examples**

In the following example, the configuration register is set to boot the system image from Flash memory:

```
config-register 0x2102
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot system</td>
<td>Specifies the system image that the router loads at startup.</td>
</tr>
<tr>
<td>confreg</td>
<td>Changes the configuration register settings while in ROM monitor mode.</td>
</tr>
<tr>
<td>o</td>
<td>Lists the value of the boot field (bits 0 to 3) in the configuration register.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.</td>
</tr>
</tbody>
</table>

### configure check syntax

To check the syntax configuration, use the `configure check syntax` command in privileged EXEC mode.

```
configure check syntax [source-location]
```

**Syntax Description**

- **source-location**: (Optional) Location or the address of the source to be checked.

**Command Default**

The syntax configuration is not checked.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to check the syntax configuration using the `configure check syntax` command:

```
Router# configure check syntax revrcsf:
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure revert</code></td>
<td>Cancels the timed rollback and triggers the rollback immediately, or resets the parameters for the timed rollback.</td>
</tr>
</tbody>
</table>

**configuration mode exclusive**

**Note**

Effective with Cisco IOS XE Release 3.1S, the `configuration mode exclusive` command is replaced by the `parser command serializer` command. See the `parser command serializer` command for more information.

To enable single-user (exclusive) access functionality for the Cisco CLI, use the `configuration mode exclusive` command in global configuration mode. To disable the single-user access (configuration locking) feature, use the `no` form of this command.

```
configuration mode exclusive {auto|manual} [expire seconds] [lock-show] [interleave] [terminate] [config-wait seconds] [retry-wait seconds]
```

```no configuration mode exclusive```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto</code></td>
<td>Automatically limits configuration to single-user mode.</td>
</tr>
<tr>
<td><code>manual</code></td>
<td>Allows you to manually limit the configuration file to single-user mode.</td>
</tr>
<tr>
<td><code>expire seconds</code></td>
<td>(Optional) Specifies the number of seconds in which the configuration lock is released after the user stops making configuration changes.</td>
</tr>
<tr>
<td><code>lock-show</code></td>
<td>(Optional) Gives priority to configuration commands being executed from the exclusive configuration session, and prevents the execution of <code>show</code> commands.</td>
</tr>
</tbody>
</table>
| `interleave` | (Optional) Allows `show` commands from sessions that are not holding the configuration lock to be executed when the user in the session holding the configuration lock is not making configuration changes.  
  **Note** If you entered the `lock-show` keyword, you should enter this keyword. |
| `terminate`  | (Optional) Causes the configuration command executed from the exclusive configuration session to terminate `show` and `clear` commands being executed in other sessions. |
**config-wait seconds** *(Optional)* Specifies the amount of time, in seconds, that a configuration command entered by a user in single user mode waits for `show` commands entered by other users to finish being executed. If the `show` command is still being executed when the timer expires and if the `terminate` option is set, the configuration command terminates the `show` command. If the configuration command completes execution before the specified number of seconds, the `show` command begins execution.

**retry-wait seconds** *(Optional)* Specifies the amount of time, in seconds, that `show` and `clear` EXEC commands will wait for a configuration command entered by a user in exclusive configuration mode to complete execution.

If the configuration command is still being executed when the specified amount of time has passed, the EXEC commands generate an error message and are terminated.

If execution of the configuration command is completed before the specified number of seconds, the EXEC commands are executed.

**Command Default**

Single-user mode is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(31)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(31)S. The following keywords were added: <code>config-wait</code>, <code>expire</code>, <code>interleave</code>, <code>lock-show</code>, <code>retry-wait</code>, and <code>terminate</code>. New functionality was added, including Access Session Locking.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was deprecated for Cisco IOS Release 15.0(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was replaced by the <code>parser command serializer</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

As of the 15.0 release, the configuration mode exclusive command is no longer available on the S and T trains.

The `configuration mode exclusive` command enables the exclusive configuration lock feature. The exclusive configuration lock allows single-user access to configuration modes using single-user configuration mode. While the device configuration is locked, no other users can enter configuration commands.

Users accessing the device using the state-full, session-based transports (telnet, Secure Shell (SSH) are able to enter single-user configuration mode. The user enters single-user configuration mode by acquiring the
exclusive configuration lock using the `configure terminal lock` privileged EXEC mode command. The configuration lock is released when the user exits configuration mode by using the `end` or `exit` command, or by pressing Ctrl-Z. While a user is in single-user configuration mode, no other users can configure the device. Users accessing Command Line Interface (CLI) options through stateless protocols (that is, the HTTP web-based user interface) cannot access single-user configuration mode. (However, an Application Programming Interface (API) allows the stateless transports to lock the configuration mode, complete its operations, and release the lock.)

### Examples

The following example shows how to configure the configuration file for single-user autoconfiguration mode by using the `configuration mode exclusive auto` command. Use the `configuration terminal` command to enter global configuration mode and lock the configuration mode exclusively. After the Cisco configuration mode is locked exclusively, you can verify this configuration by entering the `show configuration lock` command.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# configuration mode exclusive auto
Device(config)# end
Device# show running-configuration
Building configuration...
Current configuration : 2296 bytes
configuration mode exclusive auto <-------- auto policy
Device# configure terminal ?
<-------- lock option not displayed when in auto policy
Device# configure terminal
<-------- acquires the lock

The configuration mode is locked exclusively. The lock is cleared after you exit from configuration mode by entering the `end` or `exit` command.

```
```
Device(config)#
Device(config)# show configuration lock

Parser Configure Lock
---------------------
Owner PID : 3
User : unknown
TTY : 0
Type : EXCLUSIVE
State : LOCKED
Class : EXPOSED
Count : 1
Pending Requests : 0
User debug info : configure terminal
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 6
Lock Expiration timer (in Sec) : 593
Device(config)#
```

```
<-------- releases the lock
Device# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
  Session idle state : TRUE
  No of exec cmds getting executed : 0
  No of exec cmds blocked : 0
  Config wait for show completion : FALSE
  Remote ip address : Unknown
  Lock active time (in Sec) : 0
  Lock Expiration timer (in Sec) : 0

The following example shows how to enable the exclusive locking feature in manual mode by using the configuration mode exclusive manual command. Once you have configured manual exclusive mode, you can lock the configuration mode by using the configure terminal lock command. In this mode, the configure terminal command does not automatically lock the parser configuration mode. The lock is cleared after you exit from configuration mode by entering the end or exit command.

Device# configure terminal

Configuration mode locked exclusively. The lock will be cleared once you exit out of configuration mode using end/exit
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# configuration mode exclusive manual

Device(config)# end

Device# show running-configuration
 | include configuration

Building configuration...
Current configuration : 2298 bytes
configuration mode exclusive manual <---- 'manual' policy
Device# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
  Session idle state : TRUE
  No of exec cmds getting executed : 0
  No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device#
Device# configure terminal ?

lock Lock configuration mode <---------- 'lock' option displayed in 'manual' policy
Device# configure terminal <---------- 'configure terminal' won't acquire lock automatically
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device(config)# end

Device# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device#
Device# configure

Device# configure terminal

Device# configure terminal ?

lock Lock configuration mode <---------- 'lock' option displayed when in 'manual' policy
Device# configure terminal lock
Device# configure terminal lock
<------------- acquires exclusive configuration lock

Configuration mode is locked exclusively. The lock is cleared after you exit from configuration mode by entering the end or exit command. Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# show configuration lock

Parser Configure Lock
---------------------
Owner PID : 3
User : unknown
TTY : 0
Type : EXCLUSIVE
State : LOCKED
Class : EXPOSED
Count : 1
Pending Requests : 0
User debug info : configure terminal lock
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 5
Lock Expiration timer (in Sec) : 594
Device(config)# end
<----------------- 'end' releases exclusive configuration lock
Device# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>debug configuration lock</td>
<td>Enables debugging of the Cisco configuration lock.</td>
</tr>
<tr>
<td>show configuration lock</td>
<td>Displays information about the lock status of the running configuration file during a configuration replace operation.</td>
</tr>
</tbody>
</table>
**configure confirm**

To confirm replacement of the current running configuration with a saved Cisco configuration file, use the `configure confirm` command in privileged EXEC mode.

```
configure confirm
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The replacement of the current running configuration with a saved configuration file is not confirmed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2SR.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2SX.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `configure confirm` command is used only if the `time seconds` keyword and argument of the `configure replace` command are specified. If the `configure confirm` command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the `configure replace` command).

**Examples**

The following example shows the use of the `configure replace` command with the `time seconds` keyword and argument. You must enter the `configure confirm` command within the specified time limit to confirm replacement of the current running configuration file:

```
Device# configure replace nvram:startup-config time 120
This will apply all necessary additions and deletions to replace the current running configuration with the contents of the specified configuration file, which is assumed to be a complete configuration, not a partial configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
Device# configure confirm
```
configure memory

To configure the system from the system memory, use the `configure memory` command in privileged EXEC mode.

configure memory

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

On all platforms except Class A Flash file system platforms, this command executes the commands located in the configuration file in NVRAM (the “startup configuration file”).

On Class A Flash file system platforms, if you specify the `configure memory` command, the router executes the commands pointed to by the CONFIG_FILE environment variable. The CONFIG_FILE environment variable specifies the location of the configuration file that the router uses to configure itself during initialization. The file can be located in NVRAM or any of the Flash file systems supported by the platform.

When the CONFIG_FILE environment variable specifies NVRAM, the router executes the NVRAM configuration only if it is an entire configuration, not a distilled version. A distilled configuration is one that does not contain access lists.

To view the contents of the CONFIG_FILE environment variable, use the `show bootvar EXEC command`. To modify the CONFIG_FILE environment variable, use the `boot config` command and then save your changes by issuing the `copy system:running-config nvram:start-up-config` command.

**Examples**

In the following example, a router is configured from the configuration file in the memory location pointed to by the CONFIG_FILE environment variable:
Router# configure memory

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).</td>
</tr>
<tr>
<td>copy system:running-config nvram:startup-config</td>
<td>Saves the running configuration as the startup configuration file.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
</tr>
</tbody>
</table>

### configure network

The `configure network` command was replaced by the `copy {rcp | tftp} running-config` command in Cisco IOS Release 11.0. To maintain backward compatibility, the `configure network` command continues to function in Cisco IOS Release 12.2(11)T for most systems, but support for this command may be removed in a future release.

The `copy {rcp | tftp} running-config` command was replaced by the `copy {ftp | rcp | tftp} [filename] system: running-config` command in Cisco IOS Release 12.1.

The `copy {ftp | rcp | tftp} [filename] system: running-config` command specifies that a configuration file should be copied from a FTP, rcp, or TFTP source to the running configuration. See the description of the `copy` command in this chapter for more information.

### configure overwrite-network

The `configure overwrite-network` has been replaced by the `copy {ftp-url | rcp-url | tftp-url nvram:startup-config` command. See the description of the `copy` command in the Cisco IOS File System Commands chapter for more information.

### configure replace

To replace the current running configuration with a saved Cisco configuration file, use the `configure replace` command in privileged EXEC mode.

```
configure replace target-url [nolock] list force ignorecase [ [revert trigger [error] [timer minutes]] time minutes] ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target-url</td>
<td>URL (accessible by the Cisco file system) of the saved Cisco configuration file that is to replace the current running configuration.</td>
</tr>
<tr>
<td>nolock</td>
<td>(Optional) Disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replace operation.</td>
</tr>
<tr>
<td>list</td>
<td>Displays a list of the command lines applied by the Cisco software parser during each pass of the configuration replace operation. The total number of passes performed is also displayed.</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>force</td>
<td>Replaces the current running configuration file with the specified saved Cisco configuration file without prompting you for confirmation.</td>
</tr>
<tr>
<td>ignorecase</td>
<td>Instructs the configuration to ignore the case of the configuration confirmation.</td>
</tr>
<tr>
<td>revert trigger</td>
<td>(Optional) Sets the triggers for reverting to the original configuration.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>error</strong> : Reverts to the original configuration upon error.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>timer minutes</strong> : Reverts to the original configuration if the specified time elapses.</td>
</tr>
<tr>
<td>time minutes</td>
<td>(Optional) Time (in minutes) within which you must enter the <code>configure confirm</code> command to confirm replacement of the current running configuration file. If the <code>configure confirm</code> command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the <code>configure replace</code> command).</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>The <strong>nolock</strong> keyword was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The <strong>revert</strong> and <strong>trigger</strong> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>The <strong>ignorecase</strong> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you are configuring more than one keyword option, the following rules apply:

- The **list** keyword must be entered before the **force** and **time** keywords.
- The **force** keyword must be entered before the **time** keyword.
If the current running configuration is replaced with a saved Cisco configuration file that contains commands that are not accepted by the Cisco software parser, an error message is displayed that lists the commands that were not accepted. The total number of passes performed in the configuration replace operation is also displayed.

In Cisco IOS Release 12.2(25)S, a locking feature for the configuration replace operation was introduced. When the `configure replace` command is enabled, the Cisco running configuration file is locked by default for the duration of the configuration replace operation. This locking mechanism prevents other users from changing the running configuration while the replace operation is taking place, which avoids the replace operation from terminating unsuccessfully. You can disable the locking of the running configuration by using the `configure replace nolock` command.

The running configuration lock is automatically cleared at the end of the configuration replace operation. You are not expected to clear the lock manually during the replace operation, but as a protection against any unforeseen circumstances, you can manually clear the lock by using the `clear configuration lock` command. You can also display any locks that are currently applied to the running configuration by using the `show configuration lock` command.

### Note

You cannot replace the controller configuration of the T1 E1 card by using the `configure replace` command.

### Replacing the Current Running Configuration with a Saved Cisco Configuration File

The following example shows how to replace the current running configuration with a saved Cisco configuration file named `disk0:myconfig`. Note that the `configure replace` command interactively prompts you to confirm the operation.

```
Device# configure replace disk0:myconfig
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
```

In the following example, the `list` keyword is specified to display the command lines that were applied during the configuration replace operation:

```
Device# configure replace disk0:myconfig list
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
!Pass 1
!List of Commands:
sno snmp-server community public ro
snmp-server community mystring ro

end
Total number of passes: 1
Rollback Done
```
Reverting to the Startup Configuration File

The following example shows how to revert to the Cisco startup configuration file. This example also shows the use of the optional force keyword to override the interactive user prompt.

Device# configure replace nvram:startup-config force
Total number of passes: 1
Rollback Done

Performing a Configuration Replace Operation with the configure confirm Command

The following example shows the use of the configure replace command with the time seconds keyword and argument. You must enter the configure confirm command within the specified time limit to confirm replacement of the current running configuration file. If the configure confirm command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the configure replace command).

Device# configure replace nvram:startup-config time 120
This will apply all necessary additions and deletions to replace the current running configuration with the contents of the specified configuration file, which is assumed to be a complete configuration, not a partial configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
Device# configure confirm

Performing a Configuration Rollback Operation

The following example shows how to make changes to the current running configuration and then rollback the changes. As a part of the configuration rollback operation, you must save the current running configuration before making changes to the file. In this example, the archive config command is used to save the current running configuration. Note that the generated output of the configure replace command indicates that only one pass was performed to complete the rollback operation.

Note

The path command must be configured before using the archive config command.

You first save the current running configuration in the configuration archive as follows:

Device# archive config

You then enter configuration changes as shown in the following example:

Device# configure terminal
Device(config)# user netops2 password rain
Device(config)# user netops3 password snow
Device(config)# exit
After making changes to the running configuration file, you should roll back these changes and revert to the configuration that was present prior to making changes. The `show archive` command is used to verify the version of the configuration that needs to be used as a target file. The `configure replace` command is then used to revert to the target configuration file as shown in the following example:

```
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
Archive  #   Name
0           disk0:myconfig-1 <- Most Recent
2
3
4
5
6
7
8
9
10
Device# configure replace disk0:myconfig-1
Total number of passes: 1
Rollback Done
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>archive config</code></td>
<td>Saves a copy of the current running configuration to the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>configure confirm</code></td>
<td>Confirms replacement of the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>path</code></td>
<td>Specifies the location and filename prefix for the files in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>show archive</code></td>
<td>Displays information about the files saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>time-period</code></td>
<td>Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.</td>
</tr>
</tbody>
</table>

### configure revert

To cancel the timed rollback and trigger the rollback immediately, or to reset the parameters for the timed rollback, use the `configure revert` command in privileged EXEC mode.

```
configure revert {now|timer {minutes|idle minutes}}
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>now</code></td>
<td>Cancels the timed rollback and reverts immediately.</td>
</tr>
<tr>
<td><code>timer</code></td>
<td>Resets the confirmation timer.</td>
</tr>
<tr>
<td><code>minutes</code></td>
<td>Time in minutes (1-120).</td>
</tr>
</tbody>
</table>
Idletimeinminutes (1-120) for which to wait before rollback.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
In order to use the **configure revert** command to configure a timed rollback, the Configuration Archive functionality must be enable first. The Configuration Archive APIs are used to store the current configuration before applying any changes or rolling back to the previous configuration.

In case of multi-user environments, only the user who enabled the timed rollback functionality will have the permission to perform the following operations:

- Confirm the configuration change
- Reset the timer
- Cancel the timer and trigger rollback immediately

**Examples**
The following example shows how to cancel the timed rollback and revert to the saved configuration immediately:

```
Device(config)# archive
Device(config-archive)# path disk0:abc
Device# configure revert now
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive config</td>
<td>Saves a copy of the current running configuration to the Cisco configuration archive.</td>
</tr>
<tr>
<td>configure replace</td>
<td>Replaces the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td>maximum</td>
<td>Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td>path (config-archive)</td>
<td>Specifies the location and filename prefix for the files in the Cisco configuration archive.</td>
</tr>
<tr>
<td>show archive</td>
<td>Displays information about the files saved in the Cisco configuration archive.</td>
</tr>
</tbody>
</table>
configure terminal

To enter global configuration mode, use the `configure terminal` command in privileged EXEC mode.

```
configure terminal
```

**Cisco IOS Releases 12.3(14)T and Subsequent Releases:**
```
configure terminal [lock]
```

**Cisco IOS Releases 12.2(33)SRC and Subsequent Releases:**
```
configure terminal [revert {timer minutes|idle minutes}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lock</td>
<td>(Optional) Locks the running configuration into exclusive configuration mode for the duration of your configuration session. This keyword only functions if the <code>configuration mode exclusive</code> command was previously enabled.</td>
</tr>
<tr>
<td>revert</td>
<td>(Optional) Sets the parameters for reverting the configuration if confirmation of the new configuration is not received.</td>
</tr>
<tr>
<td>timer minutes</td>
<td>Time in minutes (1-120) for which to wait for confirmation.</td>
</tr>
<tr>
<td>idle minutes</td>
<td>Idle time in minutes (1-120) for which to wait for confirmation.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>lock</code> keyword option was added.</td>
</tr>
<tr>
<td>12.0(31)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(31)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The <code>revert</code> keyword option was added, along with the timer parameters of <code>idle</code> and <code>minutes</code>.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use this command to enter global configuration mode. Note that commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key/Carriage Return).

After you enter the `configure terminal` command, the system prompt changes from `<device-name>>#` to `<device-name> >(config)#`, indicating that the device is in global configuration mode. To leave global configuration mode and return to privileged EXEC mode, type `exit` or press Ctrl-Z.

To view the changes to the configuration you have made, use the `more system:running-config` command or `show running-config` command in user EXEC or privileged EXEC mode.

Configuration Locking

The first user to enter the `configure terminal lock` command acquires the configuration lock (exclusive configuration mode).

Examples

The following example shows how to enter global configuration mode and lock the Cisco software in exclusive mode:

```
Device(config)# configure terminal lock
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the device configures itself during initialization (startup).</td>
<td></td>
</tr>
<tr>
<td>configuration mode exclusive</td>
<td>Enables locking of the configuration file for single user access.</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Saves the running configuration as the startup configuration file.</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>copy system:running-config nvravm:startup-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the currently running configuration.</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>more system:running-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

confreg

To change the configuration register settings while in ROM monitor mode, use the `confreg` command in ROM monitor mode.

```
confreg [value]
```

Syntax Description

| value | (Optional) Hexadecimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF. |
Command Default

Refer to your platform documentation for the default configuration register value.

Command Modes

ROM monitor

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Not all versions in the ROM monitor support this command. Refer to your platform documentation for more information on ROM monitor mode.

If you use this command without specifying the configuration register value, the router prompts for each bit of the configuration register.

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.

To change the boot field value and leave all other bits set to their default values, follow these guidelines:

- If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the `boot` command.
- If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.
- If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.

For more information about the configuration register bit settings and default filenames, refer to the appropriate router hardware installation guide.

Examples

In the following example, the configuration register is set to boot the system image from Flash memory:

```
confreg 0x210F
```

In the following example, no configuration value is entered, so the system prompts for each bit in the register:

```
rommon ? > conreg

    Configuration Summary
    enabled are:
    console baud: 9600
    boot: the ROM Monitor

do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]: y
enable "use net in IP bcast address"? y/n [n]:
enable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]: y
```
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400 [0]: 0
change the boot characteristics? y/n [n]: y
enter to boot:
0 = ROM Monitor
1 = the boot helper image
2-15 = boot system
[0]: 0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n [n]:
You must reset or power cycle for new config to take effect.
rommon 8>

continue (ROM monitor)

To return to EXEC mode from ROM monitor mode, use the continue command in ROM monitor mode.

```
continue
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

ROM monitor

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to return to EXEC mode from ROM monitor mode, to use the system image instead of reloading. On older platforms, the angle bracket (<>) indicates that the router is in ROM monitor mode. On newer platforms, rommon number> is the default ROM monitor prompt. Typically, the router is in ROM monitor mode when you manually load a system image or perform diagnostic tests. Otherwise, the router will most likely never be in this mode.

**Caution**

While in ROM monitor mode, the Cisco IOS system software is suspended until you issue either a reset or the continue command.

**Examples**

In the following example, the continue command switches the router from ROM monitor to EXEC mode:

```
> continue
Router#`

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>Boots the router manually.</td>
</tr>
</tbody>
</table>

**copy**

To copy any file from a source to a destination, use the `copy` command in privileged EXEC or diagnostic mode. Please note that the `copy` command does not yet support the handling of wildcards in order to specify multiple files as part of source-url.

`copy [erase] [{/verify|noverify}] source-url destination-url`

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/erase</code></td>
<td>(Optional) Erases the destination file system before copying.</td>
</tr>
<tr>
<td>Note</td>
<td>This option is typically provided on platforms with limited memory to allow for an easy way to clear local flash memory space.</td>
</tr>
<tr>
<td><code>/verify</code></td>
<td>(Optional) Verifies the digital signature of the destination file. If verification fails, the file is deleted from the destination file system. This option applies to Cisco IOS software image files only.</td>
</tr>
<tr>
<td><code>/noverify</code></td>
<td>(Optional) If the file being copied is an image file, this keyword disables the automatic image verification that occurs after an image is copied.</td>
</tr>
<tr>
<td>Note</td>
<td>This keyword is often issued if the <code>file verify auto</code> command is enabled, which automatically verifies the digital signature of all images that are copied.</td>
</tr>
<tr>
<td><strong>source-url</strong></td>
<td>The location URL (or alias) of the source file or directory to be copied. The source can be either local or remote, depending upon whether the file is being downloaded or uploaded.</td>
</tr>
<tr>
<td><strong>destination-url</strong></td>
<td>The destination URL (or alias) of the copied file or directory. The destination can be either local or remote, depending upon whether the file is being downloaded or uploaded.</td>
</tr>
</tbody>
</table>

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or a filename that follows the standard Cisco IOS file system syntax (`filesystem :[/filepath ][/filename ]`).

The table below shows two keyword shortcuts to URLs.

**Table 11: Common Keyword Aliases to URLs**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>running-config</strong></td>
<td>(Optional) Keyword alias for the <code>system:running-config</code> URL. The <code>system:running-config</code> keyword represents the current running configuration file. This keyword does not work in <code>more</code> and <code>show file</code> EXEC command syntaxes.</td>
</tr>
</tbody>
</table>
The nvram:startup-config keyword represents the configuration file used during initialization (startup). This file is contained in NVRAM for all platforms except the Cisco 7000 family, which uses the CONFIG_FILE environment variable to specify the startup configuration. The Cisco 4500 series cannot use the copy running-config startup-config command. This keyword does not work in more and show file EXEC command syntaxes.

The following tables list URL prefix keywords by file system type. The available file systems will vary by platform. If you do not specify a URL prefix keyword, the router looks for a file in the current directory.

Table 12: URL Prefix Keywords for Special File Systems

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>cns:</td>
<td>Source URL for Cisco Networking Services files.</td>
</tr>
<tr>
<td>flh:</td>
<td>Source URL for flash load helper log files.</td>
</tr>
<tr>
<td>logging</td>
<td>Source URL which copies messages from the logging buffer to a file.</td>
</tr>
<tr>
<td>modem:</td>
<td>Destination URL for loading modem firmware on to supported networking devices.</td>
</tr>
<tr>
<td>null:</td>
<td>Null destination for copies or files. You can copy a remote file to null to determine its size.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.</td>
</tr>
<tr>
<td>obfl:</td>
<td>Source or destination URL for Onboard Failure Logging files.</td>
</tr>
<tr>
<td>stby-nvram:</td>
<td>Router NVRAM on the standby hardware. You can copy the startup configuration to NVRAM or from NVRAM.</td>
</tr>
<tr>
<td>stby-obfl:</td>
<td>Source or destination URL for Onboard Failure Logging files on the standby hardware.</td>
</tr>
<tr>
<td>system:</td>
<td>Source or destination URL for system memory, which includes the running configuration.</td>
</tr>
<tr>
<td>tar:</td>
<td>Source URL for the archive file system.</td>
</tr>
<tr>
<td>tmpsys:</td>
<td>Source or destination URL for the temporary system files.</td>
</tr>
<tr>
<td>xmodem:</td>
<td>Source or destination for a file from a network machine that uses the Xmodem protocol.</td>
</tr>
<tr>
<td>ymodem:</td>
<td>Source or destination for a file from a network machine that uses the Ymodem protocol.</td>
</tr>
</tbody>
</table>

The table below lists URL prefix keywords for remote file systems.

Table 13: URL Prefix Keywords for Remote File Systems

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp:</td>
<td>Source or destination URL for FTP network server. The syntax for this alias is as follows: ftp:][/username:[password]@location/directory]/filename.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Source or Destination</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>http://</td>
<td>Source or destination URL for an HTTP server (also called a web server). The syntax for this alias is as follows: http://[[username:password]@[hostname</td>
</tr>
<tr>
<td>https://</td>
<td>Source or destination URL for a Secure HTTP (HTTPS) server. HTTPS uses Secure Socket Layer (SSL) encryption. The syntax for this alias is as follows: https://[[username:password]@[hostname</td>
</tr>
<tr>
<td>rcp:</td>
<td>Source or destination URL for a remote copy protocol (rcp) network server. The syntax for this alias is as follows: rcp://[[/username@]location]/directory]/filename</td>
</tr>
<tr>
<td>scp:</td>
<td>Source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). The syntax for this alias is as follows: scp://username@location[/directory]][/filename]</td>
</tr>
<tr>
<td>tftp:</td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is as follows: tftp://[[/location]/directory]/filename</td>
</tr>
</tbody>
</table>

The table below lists URL prefix keywords for local writable storage file systems.

**Table 14: URL Prefix Keywords for Local Writable Storage File Systems**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>Source or destination URL for boot flash memory.</td>
</tr>
<tr>
<td>disk0: and disk1:</td>
<td>Source or destination URL of disk-based media.</td>
</tr>
<tr>
<td>flash:</td>
<td>Source or destination URL for flash memory. This alias is available on all platforms. For platforms that lack a flash: device, note that flash: is aliased to slot0:, allowing you to refer to the main flash memory storage area on all platforms.</td>
</tr>
<tr>
<td>harddisk:</td>
<td>Source or destination URL of the active harddisk file system.</td>
</tr>
<tr>
<td>slavebootflash:</td>
<td>Source or destination URL for internal flash memory on the slave RSP card of a router configured for HSA.</td>
</tr>
<tr>
<td>slaveram:</td>
<td>NVRAM on a slave RSP card of a router configured for HSA.</td>
</tr>
<tr>
<td>slaveslot0:</td>
<td>Source or destination URL of the first Personal Computer Memory Card International Association (PCMCIA) card on a slave RSP card of a router configured for HSA.</td>
</tr>
<tr>
<td>slaveslot1:</td>
<td>Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA.</td>
</tr>
<tr>
<td>slot0:</td>
<td>Source or destination URL of the first PCMCIA flash memory card.</td>
</tr>
<tr>
<td>slot1:</td>
<td>Source or destination URL of the second PCMCIA flash memory card.</td>
</tr>
<tr>
<td>stby-bootflash:</td>
<td>Source or destination URL for boot flash memory in standby RP.</td>
</tr>
<tr>
<td>stby-harddisk:</td>
<td>Source or destination URL for the standby harddisk.</td>
</tr>
</tbody>
</table>
### Alias | Source or Destination
---|---
stby-usb [ 0-1 ] : | Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the standby RP.

usb [ 0-1 ] : | Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the active RP.

usbflash 0 9 : | Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router.

usbtoken [0 9] : | Source or destination URL for the USB eToken that has been plugged into the router.

---

### Command Modes
- Privileged EXEC (#)
- Diagnostic (diag)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>• The http:// and https:// keywords were added as supported remote source locations (file system URL prefixes) for files.&lt;br&gt;• This command was enhanced to support copying files to servers that support SSH and the scp.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>The /verify and /noverify keywords were added.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>The /verify and /noverify keywords were integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The /verify and /noverify keywords were integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>The http:// and https:// keywords were enhanced to support file uploads.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The usbflash 0 9 : and usbtoken 0 9 : keywords were added to support USB storage.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into the Cisco 7200VXR NPE-G2 platform.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>The Cisco ASR1000 series routers became available, and introduced the copy command in diagnostic mode.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>The command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>
The fundamental function of the `copy` command is to allow you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file is specified using a Cisco IOS File System URL, which allows you to specify any supported local or remote file location. The file system being used (such as a local memory source, or a remote server) dictates the syntax used in the command.

**Usage Guidelines**

**Note**

The `copy` command copies only one file at a time. The command does not allow you to copy multiple files.

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter the `copy` command and have the router prompt you for any missing information.

For local file systems, two commonly used aliases exist for the `system:running-config` and `nvram:startup-config` files; these aliases are `running-config` and `startup-config`, respectively.

Any software that supports RFC1738 does not allow user name, path, or filename with pattern `%xy`, where (where x and y are any two hexa values 0-f, 0-F)

**Timesaver**

Aliases are used to reduce the amount of typing you need to perform. For example, it is easier to type `copy run start` (the abbreviated form of the `copy running-config startup-config` command) than it is to type `copy system:running-config nvram:startup-config`. These aliases also allow you to continue using some of the common commands used in previous versions of Cisco IOS software.

**Note**

When authorization is turned on for the `copy filesystem:/[filepath]/[filename]` `running-config` command, only the `copy` command is authorized. The individual commands available in the copied file are not authorized.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

The colon is required after the file system URL prefix keywords (such as `flash`). In some cases, file system prefixes that did not require colons in earlier software releases are allowed for backwards compatibility, but use of the colon is recommended.

In the URL syntax for `ftp:`, `http:`, `https:`, `rcp:`, `scp:`, and `tftp:`, the location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers.

The following sections contain usage guidelines for the following topics:

**Understanding Invalid Combinations of Source and Destination**

Some invalid combinations of source and destination exist. Specifically, you cannot copy:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the `copy flash: flash:` command is invalid)

**Understanding Character Descriptions**
The table below describes the characters that you may see during processing of the `copy` command.

**Table 15: copy Character Descriptions**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>!</code></td>
<td>For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).</td>
</tr>
<tr>
<td><code>.</code></td>
<td>For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.</td>
</tr>
<tr>
<td><code>O</code></td>
<td>For network transfers, an uppercase O indicates that a packet was received out of order and the copy process may fail.</td>
</tr>
<tr>
<td><code>e</code></td>
<td>For flash erasures, a lowercase e indicates that a device is being erased.</td>
</tr>
<tr>
<td><code>E</code></td>
<td>An uppercase E indicates an error. The copy process may fail.</td>
</tr>
<tr>
<td><code>V</code></td>
<td>A series of uppercase Vs indicates the progress during the verification of the image checksum.</td>
</tr>
</tbody>
</table>

Understanding Partitions

You cannot copy an image or configuration file to a flash partition from which you are currently running. For example, if partition 1 is running the current system image, copy the configuration file or image to partition 2. Otherwise, the copy operation will fail.

You can identify the available flash partitions by entering the `show file system` EXEC command.

Using rcp

The rcp requires a client to send a remote username upon each rcp request to a server. When you copy a configuration file or image between the router and a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The remote username specified in the `copy` command, if a username is specified.
2. The username set by the `ip rcmd remote-username` global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the `username` command, the router software sends the Telnet username as the remote username.
4. The router host name.

For the rcp copy request to process, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command will not run. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that username as the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, add an entry to the `rhosts` file for the remote user on the rcp server. Suppose the router contains the following configuration lines:
hostname Rtr1
ip rcmd remote-username User0

If the router IP address translates to Router1.company.com, then the .rhosts file for User0 on the rcp server should contain the following line:

Router1.company.com Rtr1

Refer to the documentation for your rcp server for more details.

If you are using a personal computer as a file server, the computer must support the remote shell protocol (rsh).

**Using FTP**

The FTP protocol requires a client to send a username and password with each FTP request to a remote FTP server. Use the `ip ftp username` and `ip ftp password` global configuration commands to specify a default username and password for all copy operations to or from an FTP server. Include the username in the `copy` command syntax if you want to specify a username for that copy operation only.

When you copy a file from the router to a server using FTP, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the `copy` command, if a username is specified.
2. The username set by the `ip ftp username` command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the `copy` command, if a password is specified.
2. The password set by the `ip ftp password` command, if the command is configured.
3. The router forms a password `username@routername.domain`. The variable `username` is the username associated with the current session, `routername` is the configured host name, and `domain` is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

---

**Note**

The Syslog message will display 'xxxx' in place of the password entered in the syntax of the `copy {ftp:}` command.

---

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that username as the remote username.

Refer to the documentation for your FTP server for details on setting up the server.

**Using HTTP or HTTPS**

Copying a file to or from a remote HTTP or HTTPS server, to or from a local file system, is performed using the embedded Secure HTTP client that is integrated in Cisco IOS software. The HTTP client is enabled by default.
Downloading files from a remote HTTP or HTTPS server is performed using the HTTP client integrated in Cisco IOS software.

If a username and password are not specified in the copy command syntax, the system uses the default HTTP client username and password, if configured.

When you copy a file from a remote HTTP or HTTPS server, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the copy command, if a username is specified.
2. The username set by the ip http client username command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the copy command, if a password is specified.
2. The password set by the ip http client password command, if the command is configured.
3. The router forms the password username@routername.domain. The variable username is the username associated with the current session, routername is the configured host name, and domain is the domain of the router.

Storing Images on Servers

Use the copy flash: destination-url command (for example, copy flash: tftp:) to copy a system image or boot image from flash memory to a network server. You can use the copy of the image as a backup copy. Also, you can also use the image backup file to verify that the image in flash memory is the same as that in the original file.

Copying from a Server to Flash Memory

Use the copy destination-url flash: command (for example, copy tftp: flash:) to copy an image from a server to flash memory.

On Class B file system platforms, the system provides an option to erase existing flash memory before writing onto it.

---

Note

Verify the image in flash memory before booting the image.

Verifying Images

When copying a new image to your router, you should confirm that the image was not corrupted during the copy process. You can verify the integrity of the image in any of the following ways:

- Depending on the destination file system type, a checksum for the image file may be displayed when the copy command completes. You can verify this checksum by comparing it to the checksum value provided for your image file on Cisco.com.
If the checksum values do not match, do not reboot the router. Instead, reissue the `copy` command and compare the checksums again. If the checksum is repeatedly wrong, copy the original image back into flash memory before you reboot the router from flash memory. If you have a corrupted image in flash memory and try to boot from flash memory, the router will start the system image contained in ROM (assuming booting from a network server is not configured). If ROM does not contain a fully functional system image, the router might not function and will need to be reconfigured through a direct console port connection.

**Caution**

- Use the `/verify` keyword.
- Enable automatic image verification by default by issuing the `file verify auto` command. This command will automatically check the integrity of each file that is copied via the `copy` command (without specifying the `/verify` option) to the router unless the `/noverify` keyword is specified.
- Use the UNIX 'diff' command. This method can also be applied to file types other than Cisco IOS images. If you suspect that a file is corrupted, copy the suspect file and the original file to a UNIX server. (The file names may need to be modified if you try to save the files in the same directory.) Then run the UNIX 'diff' command on the two files. If there is no difference, then the file has not been corrupted.

### Copying a Configuration File from a Server to the Running Configuration

Use the `copy {ftp: | rcp: | scp: | tftp:} running-config` command to load a configuration file from a network server to the running configuration of the router. (Note that `running-config` is the alias for the `system:running-config` keyword.) The configuration will be added to the running configuration as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file will be a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

You can copy either a host configuration file or a network configuration file. Accept the default value of `host` to copy and load a host configuration file containing commands that apply to one network server in particular. Enter `network` to copy and load a network configuration file containing commands that apply to all network servers on a network.

### Copying a Configuration File from a Server to the Startup Configuration

Use the `copy {ftp: | rcp: | scp: | tftp:} nvram:startup-config` command to copy a configuration file from a network server to the router startup configuration. These commands replace the startup configuration file with the copied configuration file.

### Storing the Running or Startup Configuration on a Server

Use the `copy system:running-config {ftp: | rcp: | scp: | tftp:}` command to copy the current configuration file to a network server using FTP, rcp, scp, or TFTP. Use the `copy nvram:startup-config {ftp: | rcp: | scp: | tftp:}` command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

### Saving the Running Configuration to the Startup Configuration

Use the `copy system:running-config nvram:startup-config` command to copy the running configuration to the startup configuration.
Some specific commands might not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a listing of these settings so you can quickly reconfigure your router after rebooting.

If you issue the `copy system:running-config nvram:startup-config` command from a bootstrap system image, a warning will instruct you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands to be lost. This warning does not appear if NVRAM contains an invalid configuration or if the previous configuration in NVRAM was generated by a bootstrap system image.

On all platforms except Class A filesystem platforms, the `copy system:running-config nvram:startup-config` command copies the currently running configuration to NVRAM.

On the Class A flash file system platforms, the `copy system:running-config nvram:startup-config` command copies the currently running configuration to the location specified by the CONFIG_FILE environment variable. This variable specifies the device and configuration file used for initialization. When the CONFIG_FILE environment variable points to NVRAM or when this variable does not exist (such as at first-time startup), the software writes the current configuration to NVRAM. If the current configuration is too large for NVRAM, the software displays a message and stops executing the command.

When the CONFIG_FILE environment variable specifies a valid device other than nvram: (that is, flash:, bootflash:, slot0:, or slot1:), the software writes the current configuration to the specified device and filename, and stores a distilled version of the configuration in NVRAM. A distilled version is one that does not contain access list information. If NVRAM already contains a copy of a complete configuration, the router prompts you to confirm the copy.

**Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables**

For the Class A flash file system platforms, specifications are as follows:

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOTLDR environment variable specifies the flash device and filename containing the rxboot image that ROM uses for booting.
- Cisco 3600 routers do not use a dedicated boot helper image (rxboot), which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the flash memory device and filename that are used as the boot helper; the default is the first system image in flash memory.

To view the contents of environment variables, use the `show bootvar` EXEC command. To modify the CONFIG_FILE environment variable, use the `boot config` global configuration command. To modify the BOOTLDR environment variable, use the `boot bootldr` global configuration command. To modify the BOOT environment variable, use the `boot system` global configuration command. To save your modifications, use the `copy system:running-config nvram:startup-config` command.

When the destination of a `copy` command is specified by the CONFIG_FILE or BOOTLDR environment variable, the router prompts you for confirmation before proceeding with the copy. When the destination is the only valid image in the BOOT environment variable, the router also prompts you for confirmation before proceeding with the copy.

**Using the Copy Command with the Dual RSP Feature**
The Dual RSP feature allows you to install two Route Switch Processor (RSP) cards in a single router on the Cisco 7507 and Cisco 7513 platforms.

On a Cisco 7507 or Cisco 7513 router configured for Dual RSPs, if you copy a file to `nvram:start-up-configuration` with automatic synchronization disabled, the system prompts whether you also want to copy the file to the slave start-up configuration. The default answer is yes. If automatic synchronization is enabled, the system automatically copies the file to the slave start-up configuration each time you use a `copy` command with `nvram:start-up-configuration` as the destination.

**Using the copy command with the ASR1000 Series Routers**

The `copy` command is available in both privileged EXEC and diagnostic mode on the Cisco ASR1000 series routers. Because the `copy` command is available in diagnostic mode, it can be used to copy all types of files between directories and remote locations even in the event of an IOS failure.

**Examples**

The following examples illustrate uses of the `copy` command:

**Verifying the Integrity of the Image Before it Is Copied Example**

The following example shows how to specify image verification before copying an image:

```
Router# copy /verify tftp://10.1.1.1/cisco/c7200-js-mz disk0:
Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/cisco/c7200-js-mz...
Loading cisco/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]
19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-mz
...................................................
...................................................................................................
...................................................................................................
.......................................Done!
Embedded Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

**Copying an Image from a Server to Flash Memory Examples**

The following examples use a `copy rcp:`, `copy tftp:`, or `copy ftp:` command to copy an image file from a server to flash memory:

**Copying an Image from a Server to Flash Memory Example**

The following example copies a system image named `file1` from the remote `rcp` server with an IP address of 172.16.101.101 to flash memory. On Class B file system platforms, the Cisco IOS software allows you to first erase the contents of flash memory to ensure that enough flash memory is available to accommodate the system image.

```
Router#
  copy rcp://netadmin@172.16.101.101/file1 flash:/file1
```
Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example

The following example copies a system image into a partition of flash memory. The system will prompt for a partition number only if there are two or more read/write partitions or one read-only and one read/write partition and dual flash bank support in boot ROMs. If the partition entered is not valid, the process terminates. You can enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (\textit{? number}) for directory display of a particular partition. The default is the first read/write partition. In this case, the partition is read-only and has dual flash bank support in boot ROM, so the system uses flash Load Helper.

Router# \texttt{copy tftp: flash:}

System flash partition information:
\begin{tabular}{rrrrrr}
Partition & Size & Used & Free & Bank-Size & State \\
\hline
1 & 4096K & 2048K & 2048K & 2048K & Read Only RXBOOT-FLH \\
2 & 4096K & 2048K & 2048K & 2048K & Read/Write Direct
\end{tabular}

[Type \texttt{?<no> for partition directory; \texttt{?} for full directory; \texttt{q} to abort]
Which partition? [default = 2]  

**** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then terminate  
the current system image to use the ROM based image for the copy.  
Routing functionality will not be available during that time.  
If you are logged in via telnet, this connection will terminate.  
Users with console access can see the results of the copy operation.  
---- ******** ----
Proceed? [confirm]

System flash directory, partition 1:
File Length Name/status  
1 3459720 master/igs-bfpx.100-4.3  
[3459784 bytes used, 734520 available, 4194304 total]  
Address or name of remote host [255.255.255.255]? 172.16.1.1

Source file name? master/igs-bfpx-100.4.3

Destination file name [default = source name]?
Loading master/igs-bfpx.100-4.3 from 172.16.1.111: ! 
Erase flash device before writing? [confirm]  
Flash contains files. Are you sure? [confirm]  
Copy 'master/igs-bfpx.100-4.3' from TFTP server  
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] \texttt{yes}
Copying an Image from a Server to a Flash Memory Card Partition Example

The following example copies the file `c3600-i-mz` from the rcp server at IP address 172.23.1.129 to the flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses, the Cisco IOS software prompts you to erase the files on the flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

```
Router# copy rcp: slot0:
PCMCIA Slot0 flash
Partition Size Used Free Bank-Size State Copy Mode
1 4096K 3068K 1027K 4096K Read/Write Direct
2 4096K 1671K 2424K 4096K Read/Write Direct
3 4096K 0K 4095K 4096K Read/Write Direct
4 4096K 3825K 270K 4096K Read/Write Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default - 1]
PCMCIA Slot0 flash directory, partition 1:
File Length Name/status
1 3142288 c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz
Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy '/tftpboot/images/c3600-i-mz' from server
    as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying checksum... OK (0xF89A)
Flash device copy took 00:00:18 [hh:mm:ss]
```

Saving a Copy of an Image on a Server Examples

The following examples use `copy` commands to copy image files to a server for storage:

Copy an Image from Flash Memory to an rcp Server Example

The following example copies a system image from flash Memory to an rcp server using the default remote username. Because the rcp server address and filename are not included in the command, the router prompts for it.

```
Router#
```
Copy an Image from Flash Memory to an SSH Server Using scp Example

The following example shows how to use scp to copy a system image from flash memory to a server that supports SSH:

Router# copy flash: c4500-ik2s-mz.scp scp://user1@host1/

Address or name of remote host [host1]? 
Destination username [user1]? 
Destination filename [c4500-ik2s-mz.scp]? 
Writing c4500-ik2s-mz.scp 
Password: 
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Before you can use the server-side functionality, SSH, authentication, and authorization must be properly configured so the router can determine whether a user is at the right privilege level. The scp server-side functionality is configured with the ip scp server enable command.

Copy an Image from a Partition of Flash Memory to a Server Example

The following example copies an image from a particular partition of flash memory to an rcp server using a remote username of netadmin1.

The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (number) for a directory display of a particular partition. The default is the first partition.

Router# configure terminal
Router# ip rcmd remote-username netadmin1
Router# end
Router# copy flash: rcp:
System flash partition information:
Partition Size Used Free Bank-Size State Copy-Mode
  1  4096K  2048K  2048K  2048K Read Only RXBOOT-FLH
  2  4096K  2048K  2048K  2048K Read/Write Direct
[Type ?<number> for partition directory; ? for full directory; q to abort]
Which partition? [1] 2
System flash directory, partition 2:
File Length Name/status
  1 3459720 master/igs-bfpx.100-4.3 [3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [ABC.CISCO.COM]? 
Source file name? master/igs-bfpx.100-4.3
Destination file name [master/igs-bfpx.100-4.3]?
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
Copy 'master/igs-bfpx.100-4.3' from Flash to server
as 'master/igs-bfpx.100-4.3'? [yes/no] yes
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
Copying an Image from a Flash Memory File System to an FTP Server Example

The following example copies the file c3600-i-mz from partition 1 of the flash memory card in slot 0 to an FTP server at IP address 172.23.1.129:

```
Router# show slot0: partition 1
PCMCIA Slot0 flash directory, partition 1:
File Length Name/status
1 1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]
Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)... OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

Copying an Image from Boot Flash Memory to a TFTP Server Example

The following example copies an image from boot flash memory to a TFTP server:

```
Router# copy bootflash:file1 tftp://192.168.117.23/file1
Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server as 'file1'? [yes/no] y
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying a Configuration File from a Server to the Running Configuration Example

The following example copies and runs a configuration file host1-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101:

```
Router# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Loading 1112 byte file host1-config: ![OK]
Router# %SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copying a Configuration File from a Server to the Startup Configuration Example

The following example copies a configuration file host2-config from a remote FTP server to the startup configuration. The IP address is 172.16.101.101, the remote username is netadmin1, and the remote password is ftppass.

```
Router#
copy ftp://netadmin1:ftppass@172.16.101.101/host2-config nvram:startup-config
Configure using rtr2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file rtr2-config:![OK]
[OK]
Router#
%SYS-5-CONFIG_NV:Non-volatile store configured from rtr2-config by FTP from 172.16.101.101

Copying the Running Configuration to a Server Example

The following example specifies a remote username of netadmin1. Then it copies the running configuration file named rtr2-config to the netadmin1 directory on the remote host with an IP address of 172.16.101.101.

Router# configure terminal
Router(config)# ip rcmd remote-username netadmin1
Router(config)#
end

Router#
copy system:running-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [Rtr2-config]?
Write file rtr2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101

Copying the Startup Configuration to a Server Example

The following example copies the startup configuration to a TFTP server:

Router#
copy nvram:startup-config tftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [rtr2-config]?
Write file rtr2-config on host 172.16.101.101?[confirm] <cr>
![OK]

Saving the Current Running Configuration Example

The following example copies the running configuration to the startup configuration. On a Class A flash file system platform, this command copies the running configuration to the startup configuration specified by the CONFIG_FILE variable.

copy system:running-config nvram:startup-config

The following example shows the warning that the system provides if you try to save configuration information from bootstrap into the system:
Router(boot)# copy system:running-config nvram:startup-config
Warning: Attempting to overwrite an NVRAM configuration written by a full system image. This bootstrap software does not support the full configuration command set. If you perform this command now, some configuration commands may be lost.
Overwrite the previous NVRAM configuration?[confirm]

Enter no to escape writing the configuration information to memory.

**Moving Configuration Files to Other Locations Examples**

On some routers, you can store copies of configuration files on a flash memory device. Five examples follow:

**Copying the Startup Configuration to a Flash Memory Device Example**

The following example copies the startup configuration file (specified by the CONFIG_FILE environment variable) to a flash memory card inserted in slot 0:

Router# copy nvram:startup-config slot0:router-config

**Copying the Running Configuration to a Flash Memory Device Example**

The following example copies the running configuration from the router to the flash memory PC card in slot 0:

Router# copy system:running-config slot0:berlin-cfg
Building configuration...
5267 bytes copied in 0.720 secs

**Copying to the Running Configuration from a Flash Memory Device Example**

The following example copies the file named ios-upgrade-1 from the flash memory card in slot 0 to the running configuration:

Router# copy slot0:4:ios-upgrade-1 system:running-config
Copy 'ios-upgrade-1' from flash device
as 'running-config'? [yes/no] yes

**Copying to the Startup Configuration from a Flash Memory Device Example**

The following example copies the router-image file from the flash memory to the startup configuration:

Router# copy flash:router-image nvram:startup-config
Copying a Configuration File from one Flash Device to Another Example

The following example copies the file running-config from the first partition in internal flash memory to the flash memory PC card in slot 1. The checksum of the file is verified, and its copying time of 30 seconds is displayed.

Router# copy flash: slot1:
System flash
Partition Size Used Free Bank-Size State Copy Mode
1 4096K 3070K 1025K 4096K Read/Write Direct
2 16384K 1671K 14712K 8192K Read/Write Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
System flash directory, partition 1:
File Length Name/status
1 3142748 dirt/images/mars-test/c3600-j-mz.latest
2 850 running-config
[3143728 bytes used, 1050576 available, 4194304 total]
PCMCIA Slot1 flash directory:
File Length Name/status
1 1711088 dirt/images/c3600-i-mz
2 850 running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config
Destination file name [running-config]? running-config
Verifying checksum for 'running-config' (file # 2)... OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'running-config' from flash: device
as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased 
[OK = 850/4194304 bytes]
Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum... OK (0x16)

Copying a File from a Remote Web Server Examples

In the following example, the file config1 is copied from a remote server to flash memory using HTTP:

Router# copy http://www.example.com:8080/configs/config1 flash:config1

In the following example, a default username and password for HTTP Client communications is configured, and then the file sample.scr is copied from a secure HTTP server using HTTPS:

Router# configure terminal
Router(config)# ip http client username joeuser
Router(config)# ip http client password letmein
Router(config)# end
Router# copy https://www.example_secure.com/scripts/sample.scr flash:
In the following example, an HTTP proxy server is specified before using the copy http:// command:

Router# configure terminal
Router(config)# ip http client proxy-server edge2 proxy-port 29
Router(config)# end
Router# copy http://www.example.com/configs/config3 flash:/configs/config3

Copying an Image from the Master RSP Card to the Slave RSP Card Example

The following example copies the router-image file from the flash memory card inserted in slot 1 of the master RSP card to slot 0 of the slave RSP card in the same router:

Router# copy slot1:router-image slaveslot0:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).</td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the system image that the router loads at startup.</td>
</tr>
<tr>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td>copy xmodem: flash:</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>copy ymodem: flash:</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file on a flash memory device.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td>erase</td>
<td>Erases a file system.</td>
</tr>
<tr>
<td>ip rcmd remote-username</td>
<td>Configures the remote username to be used when requesting a remote copy using rcp.</td>
</tr>
<tr>
<td>ip scp server enable</td>
<td>Enables scp server-side functionality.</td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the operating system.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
</tr>
<tr>
<td>show (flash file system)</td>
<td>Displays the layout and contents of a flash memory file system.</td>
</tr>
<tr>
<td>slave auto-sync config</td>
<td>Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Backup.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>verify bootflash:</td>
<td>File system or directory containing the files to list, followed by a colon.</td>
</tr>
</tbody>
</table>

**copy erase flash**

The `copy erase flash` command has been replaced by the `erase flash:` command. See the description of the `erase` command for more information.

On some platforms, use can use the `copy /erase source-url flash:` syntax to erase the local Flash file system before copying a new file into Flash. See the description of the `copy` command for details on this option.

**copy http**

The `copy http://` command is documented as part of the `copy` command.

**copy https**

The `copy https://` command is documented as part of the `copy` command.

**copy logging system**

To copy archived system events to a destination file system, use the `copy logging system` command in privileged EXEC mode. To stop copying the archived system events, use the `no` form of the command.

```
copy logging system target: filename
no copy logging system
```
Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>Specifies the destination file system; Valid values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• bootflash:</td>
</tr>
<tr>
<td></td>
<td>• disk0:</td>
</tr>
<tr>
<td></td>
<td>• disk1:</td>
</tr>
<tr>
<td></td>
<td>• ftp:</td>
</tr>
<tr>
<td></td>
<td>• http:</td>
</tr>
<tr>
<td></td>
<td>• https:</td>
</tr>
<tr>
<td></td>
<td>• rcp:</td>
</tr>
<tr>
<td></td>
<td>• slavebootflash:</td>
</tr>
<tr>
<td></td>
<td>• slavedisk0:</td>
</tr>
<tr>
<td></td>
<td>• slavedisk1:</td>
</tr>
<tr>
<td></td>
<td>• slavesup-bootdisk:</td>
</tr>
<tr>
<td></td>
<td>• slavesup-bootflash:</td>
</tr>
<tr>
<td></td>
<td>• sup-bootdisk:</td>
</tr>
<tr>
<td></td>
<td>• sup-bootflash:</td>
</tr>
<tr>
<td></td>
<td>• tftp:</td>
</tr>
</tbody>
</table>

filename Name of the file.

Command Default
This command has no default settings.

Command Modes
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was introduced for the Cisco uBR10012 router in the Cisco IOS Software Release 12.2(33)SCC.</td>
</tr>
</tbody>
</table>

Usage Guidelines
System Event Archive (SEA) is supported on switches that have a Supervisor Engine 32 or Supervisor Engine 720 with a compact flash adapter and a Compact Flash card (WS-CF-UPG= for Supervisor Engine 720).

**Cisco Universal Broadband Router 10012**

The System Event Archive (SEA) feature is used to address the debug trace and system console constraints. Use the `copy logging system` command to copy the major and critical events stored in the `sea_log.dat` file, to the destination file system.
To store the system event logs, the SEA requires either the PCMCIA ATA disk or Compact Flash Disk in compact flash adapter for PRE2.

The following example shows how to copy the SEA to the file system of disk0:

Router# copy logging system disk0:
Destination filename [sea_log.dat]?

The following example shows how to copy the SEA using the remote file copy function (rcp):

Router# copy logging system rcp:
Address or name of remote host []? 192.0.2.1
Destination username [Router]? username1
Destination filename [sea_log.dat]? /auto/tftpboot-users/username1/sea_log.dat

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging system</td>
<td>Clears the event records stored in the SEA.</td>
</tr>
<tr>
<td>logging system</td>
<td>Enables or disables SEA logging system.</td>
</tr>
<tr>
<td>show logging system</td>
<td>Displays the SEA logging system disk.</td>
</tr>
</tbody>
</table>

---

**copy xmodem**

To copy a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol, use the `copy xmodem: command` in EXEC mode.

`copy xmodem: flashfilesystem:`

**Syntax Description**

| flashfilesystem            | Destination of the copied file, followed by a colon. |

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is a form of the `copy` command. The `copy xmodem:` and `copy xmodem` commands are identical. See the description of the `copy` command for more information.

Copying a file using FTP, rcp, or TFTP is much faster than copying a file using Xmodem. Use the `copy xmodem:` command only if you do not have access to an FTP, TFTP, or rcp server.
This copy operation is performed through the console or AUX port. The AUX port, which supports hardware flow control, is recommended.

No output is displayed on the port over which the transfer is occurring. You can use the `logging buffered` command to log all router messages sent to the console port during the file transfer.

**Examples**

The following example initiates a file transfer from a local or remote computer to the router’s internal Flash memory using the Xmodem protocol:

```
copy xmodem: flash:
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy</code></td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td><code>copy ymodem:</code></td>
<td>Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol.</td>
</tr>
</tbody>
</table>

**copy ymodem**

To copy a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol, use the `copy ymodem:` command in EXEC mode.

```
copy ymodem: flashfilesystem:
```

**Syntax Description**

- `flashfilesystem`: Destination of the copied file, followed by a colon.

**Command Modes**

- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `copy ymodem:` and `copy ymodem` commands are identical. See the description of the `copy` command for more information.

Copying a file using FTP, rcp, or TFTP is much faster than copying a file using Ymodem. Use the `copy ymodem:` command only if you do not have access to an FTP, rcp, or TFTP server.

This copy operation is performed through the console or AUX port. The AUX port, which supports hardware flow control, is recommended.
No output is displayed on the port over which the transfer is occurring. You can use the `logging buffered` command to log all router messages sent to the console port during the file transfer.

**Examples**

The following example initiates a file transfer from a local or remote computer to the router’s internal Flash memory using the Ymodem protocol:

```
copy ymodem: flash:
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy xmodem:</code></td>
<td>Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol.</td>
</tr>
</tbody>
</table>

**copy noverify**

To disable the automatic image verification for the current copy operation, use the `copy /noverify` command.

```
copy /noverify source-url destination-url
```

**Syntax Description**

<table>
<thead>
<tr>
<th>source-url</th>
<th>Location URL or alias of the source file or directory to be copied; see the “Usage Guidelines” section for additional information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-url</td>
<td>Destination URL or alias of the copied file or directory; see the “Usage Guidelines” section for additional information.</td>
</tr>
</tbody>
</table>

**Command Default**

Verification is done automatically after completion of a copy operation.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).
Aliases are used to cut down on the amount of typing that you need to perform. For example, it is easier to type `copy run start` (the abbreviated form of the `copy running-config startup-config` command) than it is to type `copy system:r nvram:s` (the abbreviated form of the `copy system running-config nvram:startup-config` command). These aliases allow you to continue using some of the common commands that are used in previous versions of Cisco IOS software.

The table below shows two keyword shortcuts to URLs.

**Table 16: Common Keyword Aliases to URLs**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>running-config</td>
<td>(Optional) Specifies the alias for the <code>system:running-config</code> URL. This keyword does not work in the <code>more</code> and <code>show file</code> command syntaxes.</td>
</tr>
<tr>
<td>startup-config</td>
<td>(Optional) Specifies the alias for the <code>nvram:startup-config</code> URL. The <code>nvram:startup-config</code> keyword represents the configuration file that is used during initialization (startup). This file is contained in NVRAM. This keyword does not work in <code>more</code> and <code>show file</code> EXEC command syntaxes.</td>
</tr>
</tbody>
</table>

The following tables list aliases by file system type. If you do not specify an alias, the system looks for a file in the current directory.

The table below lists the URL prefix aliases for special (opaque) file systems.

**Table 17: URL Prefix Aliases for Special File Systems**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>flh:</td>
<td>Source URL for Flash load helper log files.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Router NVRAM. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file.</td>
</tr>
<tr>
<td>null:</td>
<td>Null destination for copies or files. You can copy a remote file to null to determine its size.</td>
</tr>
<tr>
<td>system:</td>
<td>Source or destination URL for system memory, which includes the running configuration.</td>
</tr>
<tr>
<td>xmodem:</td>
<td>Source destination for the file from a network device that uses the Xmodem protocol.</td>
</tr>
<tr>
<td>ymodem:</td>
<td>Source destination for the file from a network device that uses the Ymodem protocol.</td>
</tr>
</tbody>
</table>

The table below lists the URL prefix aliases for network file systems.

**Table 18: URL Prefix Aliases for Network File Systems**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp:</td>
<td>Source or destination URL for an FTP network server. The syntax for this alias is as follows: <code>ftp://[username [:password]@]location[/directory[/filename]]</code>.</td>
</tr>
<tr>
<td>Alias</td>
<td>Source or Destination</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rcp:</td>
<td>Source or destination URL for an rcp network server. The syntax for this alias is as follows: rcp:[//[username@ ] location]/directory]/filename.</td>
</tr>
<tr>
<td>tftp:</td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is tftp:[//[location]/directory]/filename.</td>
</tr>
</tbody>
</table>

The table below lists the URL prefix aliases for local writable storage file systems.

**Table 19: URL Prefix Aliases for Local Writable Storage File Systems**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>Source or destination URL for boot flash memory.</td>
</tr>
<tr>
<td>disk0: and disk1:</td>
<td>Source or destination URL of rotating media.</td>
</tr>
<tr>
<td>flash:</td>
<td>Source or destination URL for Flash memory. This alias is available on all platforms. For platforms that lack a Flash: device, note that flash: is aliased to slot0:, allowing you to refer to the main Flash memory storage area on all platforms.</td>
</tr>
<tr>
<td>slavebootflash:</td>
<td>Source or destination URL for internal Flash memory on the slave RSP card of a device that is configured for HSA.</td>
</tr>
<tr>
<td>slaveram:</td>
<td>NVRAM on a slave RSP card of a device that is configured for HSA.</td>
</tr>
<tr>
<td>slavedisk0:</td>
<td>Source or destination URL of the first PCMCIA card on a slave RSP card of a device that is configured for HSA.</td>
</tr>
<tr>
<td>slavedisk1:</td>
<td>Source or destination URL of the second PCMCIA slot on a slave RSP card of a device that is configured for HSA.</td>
</tr>
<tr>
<td>slaveslot0:</td>
<td>Source or destination URL of the first PCMCIA card on a slave RSP card of a router configured for HSA--Available on systems that are configured with a Supervisor Engine 2.</td>
</tr>
<tr>
<td>slaveslot1:</td>
<td>Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA--Available on systems that are configured with a Supervisor Engine 2.</td>
</tr>
<tr>
<td>slot0:</td>
<td>Source or destination URL of the first PCMCIA Flash memory card--Available on systems that are configured with a Supervisor Engine 2.</td>
</tr>
<tr>
<td>slot1:</td>
<td>Source or destination URL of the second PCMCIA Flash memory card--Available on systems that are configured with a Supervisor Engine 2.</td>
</tr>
</tbody>
</table>

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter the `copy` command and have the switch prompt you for any missing information.

If you enter information, choose one of the following three options: running-config, startup-config, or a file system alias (see the tables above). The location of a file system dictates the format of the source or destination URL.
The colon is required after the alias. However, earlier commands that do not require a colon remain supported but are unavailable in context-sensitive help.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

In the alias syntax for `ftp`, `rcp`, and `tftp`, the location is either an IP address or a hostname. The filename is specified for the directory that is used for file transfers.

Enter the `file verify auto` command to set up verification globally.

**Examples**

This example shows how to disable the automatic image verification for the current copy operation:

```
Router# copy /noverify tftp: sup-bootflash:
..................................................
[OK - 24301348 bytes]
24301348 bytes copied in 157.328 secs (154463 bytes/sec)
Router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>file verify auto</code></td>
<td>Verifies the compressed Cisco IOS image checksum.</td>
</tr>
<tr>
<td><code>verify</code></td>
<td>Verifies the checksum of a file on a Flash memory file system or compute an MD5 signature for a file.</td>
</tr>
</tbody>
</table>
copy noverify
D through E

- D through E, on page 130
D through E

databits

To set the number of data bits per character that are interpreted and generated by the router hardware, use the `databits` command in line configuration mode. To restore the default value, use the `no` form of the command.

```
databits \{5|6|7|8\}
no databits
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Five data bits per character.</td>
</tr>
<tr>
<td>6</td>
<td>Six data bits per character.</td>
</tr>
<tr>
<td>7</td>
<td>Seven data bits per character.</td>
</tr>
<tr>
<td>8</td>
<td>Eight data bits per character. This is the default.</td>
</tr>
</tbody>
</table>

**Command Default**

Eight data bits per character

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `databits` line configuration command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity generation is in effect, specify 8 data bits per character. The other keywords are supplied for compatibility with older devices and generally are not used.

**Examples**

The following example sets the number of data bits per character to seven on line 4:

```
Router(config)# line 4
Router(config-line)# databits 7
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-character-bits</td>
<td>Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.</td>
</tr>
<tr>
<td>terminal databits</td>
<td>Changes the number of data bits per character for the current terminal line for this session.</td>
</tr>
</tbody>
</table>
**data-character-bits**

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software, use the `data-character-bits` command in line configuration mode. To restore the default value, use the `no` form of this command.

```plaintext
data-character-bits {7/8}
no data-character-bits
```

**Syntax Description**

- **7**: Seven data bits per character.
- **8**: Eight data bits per character. This is the default.

**Command Default**

Eight data bits per character

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `data-character-bits` line configuration command is used primarily to strip parity from X.25 connections on routers with the protocol translation software option. The `data-character-bits` line configuration command does not work on hard-wired lines.

**Examples**

The following example sets the number of data bits per character to seven on virtual terminal line (vty) 1:

```plaintext
Router(config)# line vty 1
Router(config-line)# data-character-bits 7
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>terminal data-character-bits</code></td>
<td>Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.</td>
</tr>
</tbody>
</table>
default-value data-character-bits

To configure the number of data bits per character that are generated and interpreted by Cisco software to either 7 bits or 8 bits, use the `default-value data-character-bits` command in global configuration mode. To disable the configured size, use the `no` form of this command.

```
default-value data-character-bits {7|8}
no default-value data-character-bits
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Selects 7 bits as the default size.</td>
</tr>
<tr>
<td>8</td>
<td>Selects 8 bits as the default size.</td>
</tr>
</tbody>
</table>

**Command Default**

8 data bits per character are generated.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the default number of data character bits to 8:

```
Router# configure terminal
Router(config)# default-value data-character-bits 8
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-value exec-character-bits</code></td>
<td>Defines the EXEC character width to either 7 bits or 8 bits.</td>
</tr>
<tr>
<td><code>default-value modem-signal</code></td>
<td>Configures the default frequency time to scan modem signals.</td>
</tr>
<tr>
<td><code>default-value special-character-bits</code></td>
<td>Configures the flow control default value from a 7-bit width to an 8-bit width.</td>
</tr>
</tbody>
</table>

**default-value exec-character-bits**

To define the EXEC character width for either 7 bits or 8 bits, use the `default-value exec-character-bits` command in global configuration mode. To restore the default value, use the `no` form of this command.
**Syntax Description**

<table>
<thead>
<tr>
<th>Ch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Selects the 7-bit ASCII character set. This is the default.</td>
</tr>
<tr>
<td>8</td>
<td>Selects the full 8-bit ASCII character set.</td>
</tr>
</tbody>
</table>

**Command Default**

7-bit ASCII character set

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configuring the EXEC character width to 8 bits allows you to add graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can also cause failures. If a user on a terminal that is sending parity enters the `help` command, an “unrecognized command” message appears because the system is reading all 8 bits, although the eighth bit is not needed for the `help` command.

**Examples**

The following example selects the full 8-bit ASCII character set for EXEC banners and prompts:

```
Router(config)# default-value exec-character-bits 8
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-value special-character-bits</code></td>
<td>Configures the flow control default value from a 7-bit width to an 8-bit width.</td>
</tr>
<tr>
<td><code>exec-character-bits</code></td>
<td>Configures the character widths of EXEC and configuration command characters.</td>
</tr>
<tr>
<td><code>length</code></td>
<td>Sets the terminal screen length.</td>
</tr>
<tr>
<td><code>terminal exec-character-bits</code></td>
<td>Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.</td>
</tr>
<tr>
<td><code>terminal special-character-bits</code></td>
<td>Changes the ASCII character widths to accept special characters for the current terminal line and session.</td>
</tr>
</tbody>
</table>

**default-value modem-interval**

To configure the default frequency time to scan modem signals, use the `default-value modem-interval` command in global configuration mode. To disable the configured frequency, use the `no` form of this command.

```
default-value modem-interval milliseconds
```
no default-value modem-interval

Syntax Description

| milliseconds | Time frequency, in milliseconds (ms). The range is from 0 to 1000. |

Command Default

The frequency time to scan modem signals is 50 ms.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to set the default time to scan the modem signal to 345 ms:

Router# configure terminal
Router(config)# default-value modem-signal 345

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-value data-character-bits</td>
<td>Configures the default size of bits handled to either 7 bits or 8 bits.</td>
</tr>
<tr>
<td>default-value exec-character-bits</td>
<td>Defines the EXEC character width to either 7 bits or 8 bits.</td>
</tr>
<tr>
<td>default-value special-character-bits</td>
<td>Configures the flow control default value from a 7-bit width to an 8-bit width.</td>
</tr>
</tbody>
</table>

default-value special-character-bits

To configure the flow control default value from a 7-bit width to an 8-bit width, use the default-value special-character-bits command in global configuration mode. To restore the default value, use the no form of this command.

default-value special-character-bits command
default-value special-character-bits {7|8}
no default-value special-character-bits

Syntax Description

| 7 | Selects the 7-bit character set. This is the default. |
| 8 | Selects the full 8-bit character set. |

Command Default

7-bit character set

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

Configuring the special character width to 8 bits allows you to add graphical and international characters in banners, prompts, and so on.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-value exec-character-bits</code></td>
<td>Defines the EXEC character width for either 7 bits or 8 bits.</td>
</tr>
<tr>
<td><code>exec-character-bits</code></td>
<td>Configures the character widths of EXEC and configuration command characters.</td>
</tr>
<tr>
<td><code>length</code></td>
<td>Sets the terminal screen length.</td>
</tr>
<tr>
<td><code>terminal exec-character-bits</code></td>
<td>Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.</td>
</tr>
<tr>
<td><code>terminal special-character-bits</code></td>
<td>Changes the ASCII character widths to accept special characters for the current terminal line and session.</td>
</tr>
</tbody>
</table>

**define interface-range**

To create an interface-range macro, use the `define interface-range` command in global configuration mode. To remove an interface-range macro, use the `no` form of this command.

`define interface-range macro-name interface-range`

**Syntax Description**

| `macro-name` | Name of the interface-range macro. |
| `interface-range` | Type of interface range. |
| • | For a list of valid values, see the “Usage Guidelines” section. |

**Command Default**

Interface-range macro is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was integrated into Cisco IOS XE Release 12.2(17d)SXB.</td>
</tr>
</tbody>
</table>
Modification Release

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.1(2)SNG</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The **define interface-range** command applies a particular configuration on multiple interfaces and creates multiple logical, and sub interfaces.
- An interface range macro name can comprise up to 32 characters.
- An interface range for a macro can accept a maximum of five ranges. However, the subinterface range for a macro accepts only one range.
- An interface range cannot span slots.
- Use the **interface-type slot|first-interface last-interface** format to enter the interface range.
- Valid values for the interface-type argument are as follows:
  - **atm** — Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **ethernet**
  - **fastethernet**
  - **ge-wan** — Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **gigabitethernet**
  - **loopback**
  - **port-channel** **interface-number** — Valid values are from 1 to 256
  - **pos** — Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **tengigabitethernet**
  - **tunnel**
  - **vlan** **vlan-id** — Valid values are from 1 to 4094

Examples

The following example shows how to create a multiple-interface macro:

```
Device(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10
```

The following example shows how to create multiple loopback interfaces:

```
Device(config)# define interface-range loopback1-10
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface range</td>
<td>Executes a command on multiple ports at the same time.</td>
</tr>
</tbody>
</table>

delete

To delete a file on a Flash memory device or NVRAM, use the **delete** command in EXEC, privileged EXEC, or diagnostic mode.

```
delete url [{/force|recursive}]
```
## Syntax Description

<table>
<thead>
<tr>
<th><strong>url</strong></th>
<th>Cisco IOS File System URL of the file to be deleted. Include the file system prefix, followed by a colon, and, optionally, the name of a file or directory. See the table below for a list of supported URLs.</th>
</tr>
</thead>
</table>
| **/force** | (Optional) Deletes the specified file or directory without prompting you for verification.  
**Note** Use this keyword with caution: the system will not ask you to confirm the file deletion. |
| **/recursive** | (Optional) Deletes all files in the specified directory, as well as the directory itself. |

### Command Modes

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The usbflash 0 9 : and usbtoken 0 9 : options were added to the list of Cisco IOS File System URLs.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
| Cisco IOS XE Release 2.1 | This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced:  
  - This command was introduced in diagnostic mode for the first time. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR1000 Series Routers.  
  - The harddisk:, obfl:, stby-bootflash: stby-harddisk:, stby-nvram:, stby-obfl:, stby-usb[0-1]:, and usb[0 1]: url options were introduced. |

### Usage Guidelines

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion. To accept the change, you may enter y, Y, or simply hit the Enter key. Entering ? will emit a help prompt.

When you delete a file in Flash memory, the software simply marks the file as deleted, but it does not erase the file. To later recover a “deleted” file in Flash memory, use the undelete EXEC command. You can delete and undelete a file up to 15 times.

To permanently delete all files marked “deleted” on a linear Flash memory device, use the squeeze EXEC command.

The table below contains a list of Cisco IOS File System URLs.
Table 20: URL File System Prefix Keywords

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Filesystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>Delete the file from boot Flash memory.</td>
</tr>
<tr>
<td>flash:</td>
<td>Delete the file from Flash memory.</td>
</tr>
<tr>
<td>hardddisk:</td>
<td>Delete the file from the harddisk file system.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Delete the from the router NVRAM.</td>
</tr>
<tr>
<td>obfl:</td>
<td>Delete the file from the onboard failure logging file system.</td>
</tr>
<tr>
<td>slot0:</td>
<td>Delete the file from the first PCMCIA Flash memory card.</td>
</tr>
<tr>
<td>stby-bootflash:</td>
<td>Delete the file from the standby bootflash file system.</td>
</tr>
<tr>
<td>stby-harddisk:</td>
<td>Delete the file from the standby harddisk file system.</td>
</tr>
<tr>
<td>stby-nvram:</td>
<td>Delete the from the router NVRAM on the standby hardware.</td>
</tr>
<tr>
<td>stby-obfl:</td>
<td>Delete the file from the onboard failure logging file system on the standby hardware.</td>
</tr>
<tr>
<td>stby-usb [ 0 - 1 ]:</td>
<td>Delete the file from the standby USB Flash drive.</td>
</tr>
<tr>
<td>usb [ 0 - 1 ];</td>
<td>Delete the file from the USB Flash drive.</td>
</tr>
<tr>
<td>usbflash 0 9 :</td>
<td>Delete the file from the USB Flash drive.</td>
</tr>
<tr>
<td>usbtoken 0 9 :</td>
<td>Delete the file from the USB eToken.</td>
</tr>
</tbody>
</table>

Examples

The following example deletes the file named test from the Flash card inserted in slot 0:

```
Router# delete slot0:test
Delete slot0:test? [confirm]
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
</tr>
<tr>
<td>squeeze</td>
<td>Permanently deletes Flash files by squeezing a Class A Flash file system.</td>
</tr>
<tr>
<td>undelete</td>
<td>Recovers a file marked “deleted” on a Class A or Class B Flash file system.</td>
</tr>
</tbody>
</table>
To perform field diagnostics on a line card, on the Gigabit Route Processor (GRP), on the Switch Fabric Cards (SFCs), and on the Clock Scheduler Card (CSC) in Cisco 12000 series Gigabit Switch Routers (GSRs), use the `diag` command in privileged EXEC mode. To disable field diagnostics on a line card, use the `no` form of this command.

**Syntax**

```plaintext
diag command diag slot-number [:halt|previous|post|verbose [wait]|wait]
no diag slot-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>slot-number</code></td>
<td>Slot number of the line card you want to test. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router. Slot numbers for the CSC are 16 and 17, and for the FSC are 18, 19, and 20.</td>
</tr>
<tr>
<td><code>halt</code></td>
<td>(Optional) Stops the field diagnostic testing on the line card.</td>
</tr>
<tr>
<td><code>previous</code></td>
<td>(Optional) Displays previous test results (if any) for the line card.</td>
</tr>
<tr>
<td><code>post</code></td>
<td>(Optional) Initiates an EPROM-based extended power-on self-test (EPOST) only. The EPOST test suite is not as comprehensive as the field diagnostics, and a pass/fail message is the only message displayed on the console.</td>
</tr>
<tr>
<td><code>verbose [wait]</code></td>
<td>(Optional) Enables the maximum status messages to be displayed on the console. By default, only the minimum status messages are displayed on the console. If you specify the optional <code>wait</code> keyword, the Cisco IOS software is not automatically reloaded on the line card after the test completes.</td>
</tr>
<tr>
<td><code>wait</code></td>
<td>(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the completion of the field diagnostic testing. If you use this keyword, you must use the <code>microcode reload slot</code> global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the GRP will recognize the line card and download the Cisco IOS software image to the line card.</td>
</tr>
</tbody>
</table>

**Command Default**

No field diagnostics tests are performed on the line card.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 GS</td>
<td>This command was introduced to support the Cisco 12000 series GSR.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `diag` command must be executed from the GRP main console port.

Perform diagnostics on the CSC only if a redundant CSC is in the router.

Diagnostics will stop and ask you for confirmation before altering the router’s configuration. For example, running diagnostics on a SFC or CSC will cause the fabric to go from full bandwidth to one-fourth bandwidth. Bandwidth is not affected by GRP or line card diagnostics.
The field diagnostic software image is bundled with the Cisco IOS software and is downloaded automatically from the GRP to the target line card prior to testing.

⚠️ **Caution**

Performing field diagnostics on a line card stops all activity on the line card. Before the `diag EXEC` 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 the tests that are performed, 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.

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, the line card remains down (that is, in an unbooted state). In most cases, you stopped the testing because you need to remove the line card or replace the line card. If that is not the case, and you want to bring the line card back up (that is, online), you must 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. In future releases this might not be the case because DRAM and SDRAM SIMM modules might be field replaceable units. For example, if the DRAM test failed you might only need to replace the DRAM on the line card.

For more information, refer to the Cisco 12000 series installation and configuration guides.

**Examples**

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3. 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 total/indiv. timeout set to 600/220 sec. message indicates that 600 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 220 seconds to complete.

```
Router# diag 3
Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 3
Running DIAG config check
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
sending cmd FDIAG-DO ALL to fdiag in slot 3
(total/indiv. timeout set to 600/220 sec.)
Field Diagnostic ****PASSED**** for slot 3

Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
last test failed was 0, error code 0
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3
Board will reload
```
Router#  

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3 in verbose mode:

Router# diag 3 verbose  

Running Diags will halt ALL activity on the requested slot. [confirm]  
Router#  

Launching a Field Diagnostic for slot 3  
Running DIAG config check  
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)  
sending cmd FDIAG-DO ALL to fdiag in slot 3  
(total/indiv. timeout set to 600/220 sec.)  
FDIAG_STAT_IN_PROGRESS: test #1 R5K Internal Cache  
FDIAG_STAT_PASS test_num 1  
FDIAG_STAT_IN_PROGRESS: test #2 Sunblock Ordering  
FDIAG_STAT_PASS test_num 2  
FDIAG_STAT_IN_PROGRESS: test #3 Dram Datapins  
FDIAG_STAT_PASS test_num 3  
Field Diags: FDIAG_STAT_DONE  
Field Diagnostic ****PASSED**** for slot 3  
Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3  
last test failed was 0, error code 0  
sending SHUTDOWN FDIAG.Quit to fdiag in slot 3  
Board will reload  

Router#  

---

**Related Commands**

<table>
<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 on the Cisco 7000 series with RSP7000, Cisco 7500 series, or Cisco 12000 series routers after all microcode configuration commands have been entered.</td>
</tr>
</tbody>
</table>

**diagnostic bootup level**

To set the diagnostic bootup level, use the **diagnostic bootup level** command in global configuration mode. To skip all diagnostic tests, use the **no** form of this command.

```
diagnostic bootup level {minimal|complete}  
no diagnostic bootup level  
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minimal</td>
<td>Specifies minimal diagnostics. See the Usage Guidelines section for additional information.</td>
</tr>
<tr>
<td>complete</td>
<td>Specifies complete diagnostics. See the Usage Guidelines section for additional information.</td>
</tr>
</tbody>
</table>
Command Default

minimal

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The two levels are as follows:

- Complete--Runs all tests.
- Minimal--Runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.

Note

Although the default is minimal, you can set the diagnostic level to complete for troubleshooting hardware problems.

In certain circumstances, you might want to skip the bootup online diagnostics completely. For example, you might skip the bootup online diagnostics to verify that a port is as bad as online diagnostics reports. To skip online diagnostic testing completely, use the no diagnostic bootup level command.

For information on the diagnostic test types, use the show diagnostic command.

The new level takes effect at the next reload or the next time that an online insertion and removal is performed.

Examples

The following example shows how to set the diagnostic bootup level:

```
Router(config)#
diagnostic bootup level complete
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic bootup level</td>
<td>Displays the coverage level for the configured bootup diagnostics.</td>
</tr>
</tbody>
</table>

**diagnostic cns**

To configure the Cisco Networking Services (CNS) diagnostics, use the diagnostic cns command in global configuration mode. To disable sending diagnostic results to the CNS event bus, use the no form of this command.

```
diagnostic cns {publish|subscribe} [subject]
```
no diagnostic cns {publish|subscribe} [subject]

Syntax Description

<table>
<thead>
<tr>
<th>publish</th>
<th>Sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscribe</td>
<td>Receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.</td>
</tr>
<tr>
<td>subject</td>
<td>(Optional) Event subject name.</td>
</tr>
</tbody>
</table>

**Command Default**

The following are the default settings for diagnostic cns:

- diagnostic cns publish cisco.cns.device.diag_results
- diagnostic cns subscribe cisco.cns.device.diag_commands

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The online diagnostics receive events by subscribing to an event subject name. The subject is the event that you subscribe (receive) or publish (generate) through the CNS bus.

The diagnostic cns publish command sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.

The diagnostic cns subscribe command receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.

**Examples**

This example shows how to enable the publishing of diagnostic results:

```
Router(config)#
diagnostic cns publish my.cns.publish
Router(config)#
```

This example shows how to receive messages from remote network applications to perform diagnostic tests or retrieve diagnostic results:

```
Router(config)#
diagnostic cns subscribe my.cns.subscribe
Router(config)#
```

This example shows how to set the default to publish:

```
Router(config)#
default
diagnostic cns publish
Router(config)#
```
diagnostic event-log size

To modify the diagnostic event log size dynamically, use the diagnostic event-log size command in global configuration mode. To return to the default settings, use the no form of this command.

**Command Syntax**
```
diagnostic event-log size size
no diagnostic event-log size
```

**Syntax Description**
- `size`: Diagnostic event-log sizes. The valid values range from 1 to 10000 entries.

**Command Default**
The event log size is 500 entries.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The events are dynamically allocated and stored in a circular queue.
You can enter either the default diagnostic event-log size command or the no diagnostic event-log size command to return to the default settings.

**Examples**
The following example shows how to set the diagnostic event-log size:

```
Router(config)#
diagnostic event-log size 600
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic events</td>
<td>Displays the event log for the diagnostic events.</td>
</tr>
</tbody>
</table>
diagnostic level

To turn on power-on diagnostic tests for the network service engines (NSEs) installed in a Cisco 7300 series router, use the **diagnostic level** command in privileged EXEC configuration mode. There is no **no** form of this command.

```
diagnostic level {power-on|bypass}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>power-on</strong></td>
<td>Power-on diagnostic tests are performed at system bootup on the NSEs.</td>
</tr>
<tr>
<td><strong>bypass</strong></td>
<td>No diagnostic tests are performed. This is the default.</td>
</tr>
</tbody>
</table>

**Command Default**

No diagnostic tests are performed.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(10)EX2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2 S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable power-on diagnostic tests to run on the installed NSEs of a Cisco 7300 series router when the system is booted. It is recommended that you issue this command only if you are experiencing problems with an NSE and are planning on rebooting the router. Issuing this command causes an increase in the boot time.

**Examples**

The following example shows how to enable diagnostic power-on tests:

```
diagnostic level power-on
```

The following sample output shows the output that is displayed upon system bootup after a power cycle or router crash:

```
.
.
.
System Power On Diagnostics
DRAM Size ....................128 MB
Testing DRAM..................Passed
Level2 Cache ..................Present
Testing Level2 Cache (256 KB)Passed
Level3 Cache .................Passed
Testing Level3 Cache (1024 KB)Passed
System Power On Diagnostics Complete
```
This output is displayed when the system is booting, not when the command is issued.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug redundancy</code></td>
<td>Enables NSE redundancy debugging.</td>
</tr>
<tr>
<td><code>show c7300</code></td>
<td>Displays the types of cards (NSE and line cards) installed in a Cisco 7300 series router.</td>
</tr>
<tr>
<td><code>show redundancy (7300)</code></td>
<td>Displays redundancy information for the active and standby NSEs.</td>
</tr>
</tbody>
</table>

### diagnostic monitor

To configure health-monitoring diagnostic testing, use the `diagnostic monitor` command in global configuration mode. To disable testing, use the `no` form of this command.

```plaintext
diagnostic monitor interval module number test {test-id|test-id-range} [all] hh:mm:ss milliseconds days
diagnostic monitor syslog
diagnostic monitor module num test {test-id|test-id-range} [all]
no diagnostic monitor {interval|syslog}
```

**Cisco UBR10012 Router**

```plaintext
diagnostic monitor {bay slot/bay|slot slot number|subslot slot/subslot} test {test-id|test-id-range} [all] hh:mm:ss milliseconds days
diagnostic monitor syslog
diagnostic monitor threshold {bay slot/bay|slot slot-no|subslot slot/subslot} test {test-id|test-id-range} [all] failure count failures [{runs|days|hours|minutes|seconds}milliseconds] window_size
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval</code></td>
<td>Sets the interval between testing.</td>
</tr>
<tr>
<td><code>module number</code></td>
<td>Specifies the module number.</td>
</tr>
<tr>
<td><code>test</code></td>
<td>Specifies a test to run.</td>
</tr>
<tr>
<td><code>test-id</code></td>
<td>Identification number for the test to run. See the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td><code>test-id-range</code></td>
<td>Range of identification numbers for tests to be run. See the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Runs all the diagnostic tests.</td>
</tr>
<tr>
<td><code>hour hh</code></td>
<td>(Optional) Specifies the number of hours between tests. See the “Usage Guidelines” section for formatting guidelines.</td>
</tr>
<tr>
<td>Command Default</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

The defaults are as follows:

- Depending on the test run, monitoring may be enabled or disabled.
- Depending on the test run, the default monitoring interval varies.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>min mm</strong></td>
<td>(Optional) Specifies the number of minutes between tests. See the “Usage Guidelines” section for formatting guidelines.</td>
</tr>
<tr>
<td><strong>second ss</strong></td>
<td>(Optional) Specifies the number of seconds between tests. See the “Usage Guidelines” section for formatting guidelines.</td>
</tr>
<tr>
<td><strong>millisec ms</strong></td>
<td>(Optional) Specifies the number of milliseconds between tests; see the “Usage Guidelines” section for formatting guidelines.</td>
</tr>
<tr>
<td><strong>syslog</strong></td>
<td>Enables system logging messages when a health-monitoring test fails.</td>
</tr>
<tr>
<td><strong>bay slot/bay</strong></td>
<td>Indicates the card slot and bay number where the diagnostic test is run periodically and monitored. The <strong>bay</strong> keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number.</td>
</tr>
<tr>
<td><strong>slot slotnumber</strong></td>
<td>Indicates the slot number of the full-height line card where the diagnostic test is run periodically and monitored. The <strong>slot</strong> keyword is used to refer a full-height line card on the router. The valid range for the slot is from 1 to 8.</td>
</tr>
<tr>
<td><strong>subslot slot/subslot</strong></td>
<td>Indicates the slot and subslot number of half-height line card on which the diagnostic test is run periodically and monitored. The <strong>subslot</strong> keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number.</td>
</tr>
<tr>
<td><strong>threshold</strong></td>
<td>Configures the failure threshold value for the specified bay, slot, or subslot.</td>
</tr>
<tr>
<td><strong>failure count failures</strong></td>
<td>Configures the count for maximum failures allowed after which the failed test results are displayed in the output of the <strong>show diagnostic results</strong> command. The range for number of allowed failures is 0 to 99.</td>
</tr>
<tr>
<td><strong>hh:mm:ss</strong></td>
<td>Hours, minutes, and seconds interval configured to run the test again.</td>
</tr>
<tr>
<td><strong>milliseconds</strong></td>
<td>Number of milliseconds between tests.</td>
</tr>
<tr>
<td><strong>days</strong></td>
<td>Number of days between tests. The valid range is from 0 to 20.</td>
</tr>
<tr>
<td><strong>runs window_size</strong></td>
<td>Number of test-run count for the failure window-size.</td>
</tr>
<tr>
<td><strong>days window_size</strong></td>
<td>Number of days for the failure window-size.</td>
</tr>
<tr>
<td><strong>hours window_size</strong></td>
<td>Number of hours for the failure window-size.</td>
</tr>
<tr>
<td><strong>minutes window_size</strong></td>
<td>Number of minutes for the failure window-size.</td>
</tr>
<tr>
<td><strong>seconds window_size</strong></td>
<td>Number of seconds for the failure window-size.</td>
</tr>
<tr>
<td><strong>milliseconds window_size</strong></td>
<td>Number of milliseconds for the failure window-size.</td>
</tr>
</tbody>
</table>
• syslog is enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was integrated into Cisco IOS Release 12.2(33)SCC to support Generic Online</td>
</tr>
<tr>
<td></td>
<td>Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router. The keywords</td>
</tr>
<tr>
<td></td>
<td>bay, slot, and subslot were added for the Cisco UBR10012 Universal Broadband Router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use these guidelines when scheduling testing:

- **test-id** -- Enter the show diagnostic **content** command to display the test ID list.
- **test-id-range** -- Enter the show diagnostic **content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- **hh** -- Enter the hours from 1 to 24.
- **mm** -- Enter the minutes from 1 to 60.
- **days** -- Enter the number of days between tests.
- **ss** -- Enter the seconds from 1 to 60.
- **ms** -- Enter the milliseconds from 1 to 1000.

Enter the `[no] diagnostic monitor test {test-id | test-id-range | all}` command to enable or disable the specified health monitoring test.

When entering the **diagnostic monitor module number test {test-id | test-id-range | all}** command, observe the following:

- **Required**
  - Isolate network traffic by disabling all connected ports and do not pump test packets during the test.
  - Remove all modules for testing FIB TCAM and SSRAM memory on the PFC of the supervisor engine.
  - Reset the system or the test module before putting the system back into the normal operating mode.

- **Recommended**
  - If the DFC module is present, remove all modules, and then reboot the system before starting the memory test on the central PFC3B of the supervisor engine.
  - Turn off all background health-monitoring tests on the supervisor engine and the modules using the **no diagnostic monitor module number test {test-id | test-id-range | all}** command.

The FIB TCAM test for central PFC3BXL or PFC3B (on the supervisor engine) takes approximately 4 hours and 30 minutes.
The FIB TCAM test for the distributed PFC3BXL or PFC3B (on the DFC module) takes approximately 16 hours.

You can run the FIB TCAM test on multiple DFC3BX modules simultaneously.

**Cisco UBR10012 Router**

The command syntax to refer a line card or SPAs is different on Cisco UBR10012 Router. The keyword is slot x for a full-height line card, slot x/y for a half-height card, and bay x/y for a SPA.

To monitor a diagnostic test periodically, you first need to configure the hours, minutes, and seconds interval to run the diagnostic test using the `diagnostic monitor interval` command. An error message is displayed, if the interval is not configured before enabling the monitoring.

To store log details for failed tests, execute the `diagnostic monitor syslog` command. A threshold value to specify the maximum count for allowed failures is configured using the `diagnostic monitor threshold` command. The failed test results can be viewed using the `show diagnostic results` command, after the number of failed test reaches the maximum number of allowed failures configured using the `diagnostic monitor threshold` command.

---

**Examples**

The following example shows how to run the specified test every 3 days:

```
Router(config)# diagnostic monitor interval module 5 test 7 09:07:05 45 3
```

The following example shows how to enable the generation of a syslog message when any health-monitoring test fails:

```
Router(config)#
diagnostic monitor syslog
```

**Cisco UBR10012 Router**

The following example shows a sample output of an error message displayed when monitoring is enabled before configuring the test interval:

```
Router(config)# diagnostic monitor bay 1/0 test 2
Aug 12 18:04:56.280: %DIAG-3-MONITOR_INTERVAL_ZERO: Bay 1/0: Monitoring interval is 0. Cannot enable monitoring for Test #2
```

The following example shows how to configure the periodic interval for running diagnostic tests on the router before enabling monitoring:

```
Router(config)# diagnostic monitor interval bay 1/0 test 2 06:00:00 100 10
```

The following example shows how to enable logging of failed messages to syslog:

```
Router(config)# diagnostic monitor bay 1/0 test 2
```

The following example shows how to enable logging of failed messages to syslog:

```
Router(config)# diagnostic monitor syslog
```

The following example shows how to configure the failure threshold value after which the failed test results are displayed in the command output for `show diagnostic results`:

```
```
Router(config)# diagnostic monitor threshold bay 1/0 test 2 failure count 10

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show diagnostic content</td>
<td>Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.</td>
</tr>
</tbody>
</table>

**diagnostic ondemand**

To configure the on-demand diagnostics, use the `diagnostic ondemand` command in privileged EXEC mode.

```
diagnostic ondemand {iteration iteration-count|action-on-failure {continue error-count|stop}}
```

**Syntax Description**

- **iteration iteration-count**
  - Sets the number of times the same test is rerun when the command is issued.
  - The valid range for iteration-count is between 1 to 999.

- **action-on-failure**
  - Sets the execution action when a failure is detected.

- **continue**
  - Continues testing when a test failure is detected.

- **stop**
  - Stops testing when a test failure is detected.

- **error-count**
  - (Optional) Number of errors that are allowed before stopping. This argument is used with the `continue` option. The valid range for error-count is from 0 to 65534.

**Command Default**

The default settings are as follows:

- **iteration-count** is 1
- **action-on-error** is `continue`
- **error-count** is 0

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Entering 0 for the `error-count` sets the number of errors that are allowed to unlimited.
**Examples**

The following example shows how to set the ondemand testing iteration count:

Router#
```
diagnostic ondemand iteration 4
```
Router#

The following example shows how to set the execution action when an error is detected:

Router#
```
diagnostic ondemand action-on-failure continue 2
```
Router#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diagnostic ondemand settings</code></td>
<td>Displays the settings for on-demand diagnostics.</td>
</tr>
</tbody>
</table>

---

**diagnostic schedule module**

To set the scheduling of test-based diagnostic testing for a specific module or schedule a supervisor engine switchover, use the `diagnostic schedule module` command in global configuration mode. To remove the scheduling, use the `no` form of this command.

```
diagnostic schedule module {module-numberslot/subslot} test
  {test-id|all|complete|minimal|non-disruptive} [per-port [port {interface-port-number|port-number-list|all}]]
  {on month dd yyyy hh:mm|daily hh:mm|weekly day-of-week hh:mm}
```

```
no diagnostic schedule module {module-numberslot/subslot} test
  {test-id|all|complete|minimal|non-disruptive} [per-port [port {interface-port-number|port-number-list|all}]]
  {on month dd yyyy hh:mm|daily hh:mm|weekly day-of-week hh:mm}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>module-number</code></td>
<td>Specifies the module number.</td>
</tr>
<tr>
<td><code>slot / subslot</code></td>
<td>Specifies the slot number of the active supervisor engine.</td>
</tr>
<tr>
<td><code>test</code></td>
<td>Specifies the diagnostic test suite attribute.</td>
</tr>
<tr>
<td><code>test-id</code></td>
<td>Identification number for the test to be run; see the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Runs all diagnostic tests.</td>
</tr>
<tr>
<td><code>complete</code></td>
<td>Selects the complete bootup test suite.</td>
</tr>
<tr>
<td><code>minimal</code></td>
<td>Selects the minimal bootup test suite.</td>
</tr>
<tr>
<td><code>non-disruptive</code></td>
<td>Selects the nondisruptive test suite.</td>
</tr>
<tr>
<td><code>per-port</code></td>
<td>Selects the per-port test suite.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>(Optional) Specifies the port to schedule testing.</td>
</tr>
<tr>
<td><code>interface-port-number</code></td>
<td>(Optional) Port number.</td>
</tr>
</tbody>
</table>
Test-based diagnostic testing for a specific module is not scheduled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was modified to support scheduled switchover for supervisor engines.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was modified to support the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The <strong>complete</strong>, <strong>minimal</strong>, <strong>non-disruptive</strong>, and <strong>per-port</strong> keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use these guidelines when scheduling testing:

- **test-id** -- Enter the `show diagnostic content` command to display the test ID list.
- **month**-- Spell out the month such as january, february ... december (either uppercase or lowercase characters).
- **dd**-- Enter the day as a two-digit number.
- **yyyy**-- Enter the year as a four-digit number.
- **hh : mm**-- Enter the time as a two-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required.
- **day-of-week**-- Spell out the day of the week, such as monday, tuesday... sunday (either uppercase or lowercase characters).

**per-port** is not supported when specifying a scheduled switchover.

You can use the `diagnostic schedule module slot / subslot test test-id` command to schedule a switchover from the active supervisor engine to the standby supervisor engine.

Enter the `show diagnostic content module slot / subslot` command to display the test ID list and look for the test ID in the ScheduleSwitchover field.
You can specify a periodic switchover (daily or weekly) or a single switchover occurrence at a specific time using these commands:

- `diagnostic schedule module slot / subslot test test-id on mm dd yyyy hh:mm`
- `diagnostic schedule module slot / subslot test test-id daily hh:mm`
- `diagnostic schedule module slot / subslot test test-id weekly day-of-week hh:mm`

**Note**
To avoid system downtime in the event that the standby supervisor engine cannot switch over the system, Cisco recommends that you schedule a switchover from the standby supervisor engine to the active supervisor engine 10 minutes after the switchover occurs.

**Examples**

The following example shows how to schedule the diagnostic testing on a specific month, date and time for a specific module:

```
Router(config)# diagnostic schedule module 1 test 5 on may 27 2010 10:30
```

The following example shows how to schedule the diagnostic testing to occur daily at a certain time for a specific module:

```
Router(config)# diagnostic schedule module 1 test 5 daily 12:25
```

The following example shows how to schedule the diagnostic testing to occur weekly on a certain day for a specific module:

```
Router(config)# diagnostic schedule module 1 test 5 weekly friday 09:23
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diagnostic content</code></td>
<td>Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.</td>
</tr>
<tr>
<td><code>show diagnostic schedule</code></td>
<td>Displays the current scheduled diagnostic tasks.</td>
</tr>
</tbody>
</table>

**diagnostic start**

To run the specified diagnostic test, use the `diagnostic start` command in privileged EXEC mode.

```
diagnostic start module num test
{test-id|test-id-range|minimal|complete|basic|per-port|non-disruptive|all} [port{numport-range|all}]
diagnostic start system test all
```

Cisco UBR10012 Universal Broadband Router

diagnostic start {bay slot/bay|slot slot-no} test
{test-id|test-id-range|all|complete|minimal|non-disruptive}
diagnostic start subslot slot/subslot test
{test-id|test-id-range|all|complete|minimal|non-disruptive}[per-port [port|numport-range|all]]
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module <code>num</code></td>
<td>Specifies the module number.</td>
</tr>
<tr>
<td>test</td>
<td>Specifies a test to run.</td>
</tr>
<tr>
<td><code>test-id</code></td>
<td>Identification number for the test to run. See the Usage Guidelines section for additional information.</td>
</tr>
<tr>
<td><code>test-id-range</code></td>
<td>Range of identification numbers for tests to run. See the Usage Guidelines section for additional information.</td>
</tr>
<tr>
<td><code>minimal</code></td>
<td>Runs minimal bootup diagnostic tests.</td>
</tr>
<tr>
<td><code>complete</code></td>
<td>Runs complete bootup diagnostic tests.</td>
</tr>
<tr>
<td><code>basic</code></td>
<td>Runs basic on-demand diagnostic tests.</td>
</tr>
<tr>
<td><code>per-port</code></td>
<td>Runs per-port level tests.</td>
</tr>
<tr>
<td><code>non-disruptive</code></td>
<td>Runs the non disruptive health-monitoring tests.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Runs all diagnostic tests.</td>
</tr>
<tr>
<td><code>port </code> num</td>
<td>(Optional) Specifies the interface port number.</td>
</tr>
<tr>
<td><code>port </code> port# range</td>
<td>(Optional) Specifies the interface port number range. See the Usage Guidelines section for additional information.</td>
</tr>
<tr>
<td><code>port </code> all</td>
<td>(Optional) Specifies all ports.</td>
</tr>
<tr>
<td><code>system test all</code></td>
<td>Runs all disruptive and nondisruptive diagnostic tests at once. All test dependencies are handled automatically.</td>
</tr>
<tr>
<td><code>bay slot/bay</code></td>
<td>Indicates the card slot and bay number where the diagnostic test is executed. The bay keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number.</td>
</tr>
<tr>
<td><code>slot slot-no</code></td>
<td>Indicates the slot number of the full-height line card where the diagnostic test is executed. The slot keyword is used to refer a full-height line card on the router. The valid range for slot is from 1 to 8.</td>
</tr>
<tr>
<td><code>subslot slot/sub-slot</code></td>
<td>Indicates the slot and subslot number of half-height line card where the diagnostic test is executed. The subslot keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17a)SX</td>
<td>This command was changed to include the <code>complete</code> and <code>basic</code> keywords.</td>
</tr>
</tbody>
</table>
Modification

Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

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

This command was changed to include the system test all keywords.

The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router. The keywords bay, slot, and subslot were added for the Cisco UBR10012 Universal Broadband Router.

### Usage Guidelines

Running all online diagnostic tests disrupts normal system operation. Reset the system after the `diagnostic start system test all` command has completed. Do not insert, remove, or power down line cards or the supervisor while the system test is running. Do not issue any diagnostic command other than the `diagnostic stop system test all` command while the system test is running. Make sure no traffic is running in background.

**Note**

Do not enter the `diagnostic start module x test all` command on systems that are configured with a DFC3A because this command causes the TCAM test to fail.

Enter the `show diagnostic content` command to display the test ID list.

Enter the `test-id-range` or `port# range` as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).

Use `diagnostic stop` command to stop the testing process.

**Cisco UBR10012 Router**

The command syntax to refer a line card or SPAs is different on Cisco UBR10012 Router. The keyword is slot x for a full-height line card, slot x/y for a half-height card, and bay x/y for a SPA.

**Note**

To start a diagnostic test on the Cisco UBR10012 Router execute the command `diagnostic stop` with the bay, slot or subslot keyword respectively.

The GOLD test cases used to poll for system errors in Cisco IOS Software Release 12.2(33)SCC are Low Latency Queueing (LLQ) drop, Cable Line Card (CLC) memory leak, and Guardian index leak tests.

### Examples

The following example shows how to run the specified diagnostic test at the specified slot:

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no] yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn(ID=5) ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn(ID=5) has completed successfully
```
This example shows how to start all online diagnostic tests:

Router# diagnostic start system test all

`* WARNING: *
* 'diagnostic start system test all' will disrupt normal system *
* operation. The system requires RESET after the command *
* 'diagnostic start system test all' has completed prior to *
* normal use. *
* *
* IMPORTANT: *
* 1. DO NOT INSERT, OIR, or POWER DOWN Linecards or *
* Supervisor while system test is running. *
* *
* 2. DO NOT ISSUE ANY DIAGNOSTIC COMMAND except *
* "diagnostic stop system test all" while system test *
* is running. *
* *
* 3. PLEASE MAKE SURE no traffic is running in background. *
**********************************************************

Do you want to continue? [no]:

Cisco UBR10012 Router

The following example shows how to run a diagnostic test with test id 2 on a SPA:

ubr-122s-1# diagnostic start bay 1/0 test 2
ubr-122s-1#
Aug 5 09:24:42.019: %DIAG-6-TEST_RUNNING: Bay 1/0: Running TestModenaLLQDrops(ID-2) ...
Aug 5 09:24:42.019: %DIAG-6-TEST_OK: Bay 1/0: TestModenaLLQDrops(ID-2) has completed successfully

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic schedule</td>
<td>Sets the diagnostic test schedule for a particular bay, slot, or subslot.</td>
</tr>
<tr>
<td>show diagnostic description</td>
<td>Provides the description for the diagnostic tests.</td>
</tr>
<tr>
<td>diagnostic stop</td>
<td>Runs the specified diagnostic test.</td>
</tr>
<tr>
<td>show diagnostic content module</td>
<td>Displays the available diagnostic tests.</td>
</tr>
<tr>
<td>diagnostic bootup level</td>
<td>Configures the diagnostic bootup level.</td>
</tr>
<tr>
<td>diagnostic event-log size</td>
<td>Modifies the diagnostic event-log size dynamically.</td>
</tr>
<tr>
<td>diagnostic monitor</td>
<td>Configures the health-monitoring diagnostic testing.</td>
</tr>
<tr>
<td>diagnostic ondemand</td>
<td>Configures the on-demand diagnostics.</td>
</tr>
<tr>
<td>show diagnostic bootup</td>
<td>Displays the configured diagnostics level at bootup.</td>
</tr>
</tbody>
</table>
### diagnostic stop

To stop the testing process, use the **diagnostic stop** command in privileged EXEC mode.

```
diagnostic stop module num
```

**Cisco UBR10012 Universal Broadband Router**

```
diagnostic stop {bay slot/bay|slot slot-no|subslot slot/subslot}
```

#### Syntax Description

<table>
<thead>
<tr>
<th>module num</th>
<th>Module number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>bay slot/bay</td>
<td>Indicates the card slot and bay number of the SPA for which the diagnostic test has stopped. The <strong>bay</strong> keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number.</td>
</tr>
<tr>
<td>slot slot-no</td>
<td>Indicates the slot number of full height line card for which the diagnostic test has to be stopped. The <strong>slot</strong> keyword is used to refer a full-height line card on the router. Valid range for the slot is from 1 to 8.</td>
</tr>
<tr>
<td>subslot slot/subslot</td>
<td>Indicates the slot and subslot number of half-height line card for which the diagnostic test has to be stopped. The <strong>subslot</strong> keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number.</td>
</tr>
</tbody>
</table>

#### Command Default

None

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router. The keywords <strong>bay</strong>, <strong>slot</strong>, and <strong>subslot</strong> were added for the Cisco UBR10012 Universal Broadband Router.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use the diagnostic start command to start the testing process.

Cisco UBR10012 Router

The command syntax to refer a line card or SPAs is different on Cisco UBR10012 Router. The keyword is slot x for a full-height line card, slot x/y for a half-height card, and bay x/y for a SPA.

Note

To stop a diagnostic test on the Cisco UBR10012 Router execute the command `diagnostic stop` with the `bay`, `slot` or `subslot` keyword respectively.

The GOLD test cases used to poll for system errors in Cisco IOS Software Release 12.2(33)SCC are Low Latency Queueing (LLQ) drop, Cable Line Card (CLC) memory leak, and line card index leak tests.

Examples

This example shows how to stop the diagnostic test process:

Router# diagnostic stop module 3
Router#

This example shows how to stop the diagnostic test process for subslot 5/0 on the Cisco UBR10012 Universal Broadband Router:

Router# diagnostic stop subslot 5/0
Router#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic schedule</td>
<td>Sets the diagnostic test schedule for a particular bay, slot, or subslot.</td>
</tr>
<tr>
<td>show diagnostic description</td>
<td>Provides the description for the diagnostic tests.</td>
</tr>
<tr>
<td>diagnostic start</td>
<td>Stops the specified diagnostic test.</td>
</tr>
<tr>
<td>show diagnostic content module</td>
<td>Displays the available diagnostic tests.</td>
</tr>
<tr>
<td>diagnostic bootup level</td>
<td>Configures the diagnostic bootup level.</td>
</tr>
<tr>
<td>diagnostic event-log size</td>
<td>Modifies the diagnostic event-log size dynamically.</td>
</tr>
<tr>
<td>diagnostic monitor</td>
<td>Configures the health-monitoring diagnostic testing.</td>
</tr>
<tr>
<td>diagnostic ondemand</td>
<td>Configures the on-demand diagnostics.</td>
</tr>
<tr>
<td>show diagnostic bootup</td>
<td>Displays the configured diagnostics level at bootup.</td>
</tr>
<tr>
<td>show diagnostic events</td>
<td>Displays the diagnostic event log.</td>
</tr>
<tr>
<td>show diagnostic ondemand settings</td>
<td>Displays the settings for the on-demand diagnostics.</td>
</tr>
<tr>
<td>show diagnostic result</td>
<td>Displays the diagnostic test results for a module.</td>
</tr>
<tr>
<td>show diagnostic schedule</td>
<td>Displays the current scheduled diagnostic tasks.</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Displays the running diagnostics tests.</td>
</tr>
</tbody>
</table>
dir

To display a list of files on a file system, use the `dir` command in EXEC, privileged EXEC, or diagnostic mode.

```
dir [/all] [/recursive] [all-systems] [filesystem:] [file-url]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/all</code></td>
<td>(Optional) Lists deleted files, undeleted files, and files with errors.</td>
</tr>
<tr>
<td><code>/recursive</code></td>
<td>(Optional) Lists files recursively.</td>
</tr>
<tr>
<td><code>all-systems</code></td>
<td>(Optional) Lists all files in all file systems on the router.</td>
</tr>
<tr>
<td><code>filesystem:</code></td>
<td>(Optional) File system or directory containing the files to list, followed by a colon.</td>
</tr>
<tr>
<td><code>file-url</code></td>
<td>(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.</td>
</tr>
</tbody>
</table>

### Command Default

When you omit the `/all` keyword, the Cisco IOS software displays only undeleted files.

### Command Modes

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3</td>
<td>This command was modified. A timestamp that shows the offset from Coordinated Universal Time (UTC) was added to the <code>dir</code> command display.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was modified. The <code>usbflash 0 9</code> and <code>ubftoken 0 9</code> options were added as available file systems.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was modified. Support for this command was implemented on the Cisco 7200VXR NPE-G2 platform.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers, and the following enhancements were introduced:</td>
</tr>
<tr>
<td></td>
<td>• The command was made available in diagnostic mode.</td>
</tr>
<tr>
<td></td>
<td>• The <code>/recursive</code> option was introduced.</td>
</tr>
<tr>
<td></td>
<td>• The file systems available with the Cisco ASR 1000 Series Routers became available as <code>filesystem:</code> options.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The output modifier was added.</td>
</tr>
<tr>
<td>15.0(01)XO</td>
<td>Note added to explain different byte and usage calculations for <code>show file systems</code> and <code>dir</code> commands on cat4000 series routers.</td>
</tr>
</tbody>
</table>
Use the `show file systems` command to display more details about the files in a particular file system.

**Note**

As of release 15.0(01)XO, on cat4000 series routers, the `show (flash file system)` and `dir` will display slightly different byte count and usage information for the same file system. This is due to slight difference in how IOS computes these figures for this platform.

You can use the Cisco IOS software output modifiers to filter the output of the `dir` command, to display only those lines you are interested in.

The output modifier feature is invoked by using the pipe symbol (|). To use this feature, enter the `dir` command as normal but add a space and the pipe symbol at the end of the command line. Then add one of the keywords shown in the table below.

**Table 21: Using Output Modifiers**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>append</code></td>
<td>Appends redirected output to URL (only to the URLs supporting the append operation).</td>
</tr>
<tr>
<td><code>begin</code></td>
<td>Displays the first line that matches the regular expression, and then all other lines that follow that line.</td>
</tr>
<tr>
<td><code>include</code></td>
<td>Displays all lines that match the regular expression.</td>
</tr>
<tr>
<td><code>exclude</code></td>
<td>Displays all lines except those that match the regular expression.</td>
</tr>
<tr>
<td><code>format</code></td>
<td>Formats the output using the specification file.</td>
</tr>
<tr>
<td><code>redirect</code></td>
<td>Redirects the output to the URL.</td>
</tr>
<tr>
<td><code>section</code></td>
<td>Filters a section of the output.</td>
</tr>
<tr>
<td><code>tee</code></td>
<td>Copies output to the URL.</td>
</tr>
</tbody>
</table>

The `append`, `redirect` and `tee` keywords do not support `rcp` in the display.

**Examples**

The following is sample output from the `dir` command:

```
Router# dir slot0:
Directory of slot0:/
1 -rw- 4720148 Dec 29 2003 17:49:36 -08:00 hampton/nitro/c7200-j-mz
2 -rw- 4767328 Jan 02 2004 18:42:53 -08:00 c7200-js-mz
5 -rw- 639 Jan 03 2004 12:09:32 -08:00 rally
7 -rw- 639 Jan 03 2004 12:37:13 -08:00 the_time
20578304 bytes total (3104544 bytes free)
```

The following is sample output from the `dir /all` command:

```
Router# dir /all slot0:
```
Directory of slot0:

1 -rw- 4720148 Dec 15 2003 17:49:36 -08:00 hampton/nitro/c7200-j-mz
2 -rw- 4767328 Jan 02 2004 18:42:53 -08:00 c7200-js-mz
3 -rw- 7982828 Jan 02 2004 18:48:14 -08:00 [rsp-jsv-mz]
4 -rw- 639 Jan 03 2004 12:09:17 -08:00 the_time]
5 -rw- 639 Jan 03 1994 12:09:32 -08:00 rally
6 -rw- 639 Jan 03 1994 12:37:01 -08:00 [the_time]
7 -rw- 639 Jan 03 1994 12:37:13 -08:00

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

### Table 22: dir Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Index number of the file.</td>
</tr>
<tr>
<td>-rw-</td>
<td>Permissions. The file can be any or all of the following:</td>
</tr>
<tr>
<td></td>
<td>• d--directory</td>
</tr>
<tr>
<td></td>
<td>• r--readable</td>
</tr>
<tr>
<td></td>
<td>• w--writable</td>
</tr>
<tr>
<td></td>
<td>• x--executable</td>
</tr>
<tr>
<td>4720148</td>
<td>Size of the file, in bytes.</td>
</tr>
<tr>
<td>Dec 15 2003 17:49:36</td>
<td>Last modification date.</td>
</tr>
<tr>
<td>-08:00</td>
<td>Conversion to local time in hours from Coordinated Universal Time (UTC). In the example, -08:00 indicates that the given time is 8 hours behind UTC or Pacific Standard Time (PST).</td>
</tr>
<tr>
<td>hampton/nitro/c7200-j-mz</td>
<td>Filename. Deleted files are indicated by square brackets around the filename.</td>
</tr>
</tbody>
</table>

The following example shows how to use the output modifier feature with the exclude keyword and regular expression. The table above describes the significant fields shown in the output.

Routwe# dir | exclude asr
Directory of bootflash:

12 drwx 4096 Jan 5 2005 01:34:50 +00:00 lost+found
59265 drwx 4096 Apr 20 2004 01:51:10 +00:00 .installer
14817 drwx 4096 Apr 20 2004 01:54:37 +00:00 .ssh
88897 drwx 4096 Jan 7 2005 22:13:26 +00:00 .prst_sync

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file on a Flash memory device.</td>
</tr>
<tr>
<td>undelete</td>
<td>Recovers a file marked “deleted” on a Class A or Class B flash file system.</td>
</tr>
</tbody>
</table>
disable

To exit privileged EXEC mode and return to user EXEC mode, or to exit to a lower privilege level, enter the disable command in EXEC, privileged EXEC, or diagnostic mode.

disable [privilege-level]

Syntax Description

| privilege-level | (Optional) Specific privilege level (other than user EXEC mode). |

Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC (&gt;)</td>
<td>Privileged EXEC mode</td>
</tr>
<tr>
<td>Privileged EXEC (#)</td>
<td>Diagnostic (diag)</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers, and became available in diagnostic mode.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Up to 16 security levels can be configured using Cisco IOS software. If such levels are configured on a system, using this command with the privilege-level option allows you to exit to a lower security level. If a level is not specified, the user will exit to the user EXEC mode, which is the default.

Note

Five EXEC commands are associated with privilege level 0: disable, enable, exit, help, and logout. If you configure a privilege level greater than 0, these five commands will not be included in the command set for that privilege level.

Examples

In the following example, the user enters privileged EXEC mode using the enable command, then exits back to user EXEC mode using the disable command. Note that the prompt for user EXEC mode is >, and the prompt for privileged EXEC mode is #.

```
Router> enable
Password: <letmein>
Router# disable
Router> 
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables higher privilege level access, such as privileged EXEC mode.</td>
</tr>
</tbody>
</table>

disconnect-character

To define a character to disconnect a session, use the disconnect-character command in line configuration mode. To remove the disconnect character, use the no form of this command.
disconnect-character  ascii-number
no  disconnect-character

Syntax Description

| ascii-number | Decimal representation of the session disconnect character. |

Command Default

No disconnect character is defined.

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

See the “ASCII Character Set and Hex Values” appendix for a list of ASCII characters. The Break character is represented by zero; NULL cannot be represented. To use the session-disconnect character in normal communications, precede it with the escape character.

Examples

The following example defines the disconnect character for virtual terminal line 4 as Escape, which is decimal character 27:

```
Router(config)# line vty 4
Router(config-line)# disconnect-character 27
```

dispatch-character

To define a character that causes a packet to be sent, use the dispatch-character command in line configuration mode. To remove the definition of the specified dispatch character, use the no form of this command.

dispatch-character  ascii-number1  [ascii-number2  . . . ]
no dispatch-character  ascii-number1  [ascii-number2  . . . ]

Syntax Description

<table>
<thead>
<tr>
<th>ascii-number1</th>
<th>Decimal representation of the desired dispatch character.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascii-number2 . . .</td>
<td>(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.</td>
</tr>
</tbody>
</table>

Command Default

No dispatch character is defined.

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

See the “ASCII Character Set and Hex Values” appendix for a list of ASCII characters.

The **dispatch-character** command defines one or more dispatch characters that cause a packet to be sent even if the dispatch timer has not expired. Use of a dispatch character causes the Cisco IOS software to attempt to buffer characters into larger-sized packets for transmission to the remote host.

Enable the **dispatch-character** command from the session that initiates the connection, not from the incoming side of a streaming Telnet session.

This command can take multiple arguments, so you can define any number of characters as dispatch characters.

Examples

The following example defines the Return character (decimal 13) as the dispatch character for virtual terminal line (vty) line 4:

```console
Router(config)# line vty 4
Router(config-line)# dispatch-character 13
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dispatch-machine</strong></td>
<td>Specifies an identifier for a TCP packet dispatch state machine on a particular line.</td>
</tr>
<tr>
<td><strong>dispatch-timeout</strong></td>
<td>Sets the character dispatch timer.</td>
</tr>
<tr>
<td><strong>state-machine</strong></td>
<td>Specifies the transition criteria for the state of a particular state machine.</td>
</tr>
<tr>
<td><strong>terminal dispatch-character</strong></td>
<td>Defines a character that causes a packet to be sent for the current session.</td>
</tr>
</tbody>
</table>

**dispatch-machine**

To specify an identifier for a TCP packet dispatch state machine on a particular line, use the **dispatch-machine** command in line configuration mode. To disable a state machine on a particular line, use the **no** form of this command.

```console
dispatch-machine name
no dispatch-machine
```

**Syntax Description**

| name                  | Name of the state machine that determines when to send packets on the asynchronous line. |

**Command Default**

No dispatch state machine identifier is defined.

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
When the `dispatch-timeout` command is specified, a packet being built will be sent when the timer expires, and the state will be reset to zero.

Any dispatch characters specified using the `dispatch-character` command are ignored when a state machine is also specified.

If a packet becomes full, it will be sent regardless of the current state, but the state will not be reset. The packet size depends on the traffic level on the asynchronous line and the dispatch-timeout value. There is always room for 60 data bytes. If the dispatch-timeout value is greater than or equal to 100 milliseconds, a packet size of 536 (data bytes) is allocated.

The following example specifies the name linefeed for the state machine:

```plaintext
Router(config)# state-machine linefeed 0 0 9 0
Router(config)# state-machine linefeed 0 11 255 0
Router(config)# state-machine linefeed 0 10 10 transmit
Router(config)# line 1
Router(config-line)# dispatch-machine linefeed
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dispatch-character</code></td>
<td>Defines a character that causes a packet to be sent.</td>
</tr>
<tr>
<td><code>dispatch-timeout</code></td>
<td>Sets the character dispatch timer.</td>
</tr>
<tr>
<td><code>state-machine</code></td>
<td>Specifies the transition criteria for the state of a particular state machine.</td>
</tr>
</tbody>
</table>

**dispatch-timeout**

To set the character dispatch timer, use the `dispatch-timeout` command in line configuration mode. To remove the timeout definition, use the `no` form of this command.

```
no dispatch-timeout
```

**Syntax Description**

| milliseconds        | Integer that specifies the number of milliseconds (ms) that the Cisco IOS software waits after putting the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host. |

**Command Default**

No dispatch timeout is defined.

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use this command to increase the processing efficiency for the remote host.

The `dispatch-timeout` line configuration command causes the software to buffer characters into packets for transmission to the remote host. The Cisco IOS software sends a packet a specified amount of time after the first character is put into the buffer. You can use the `dispatch-timeout` and `dispatch-character` line configuration commands together. In this case, the software dispatches a packet each time the dispatch character is entered, or after the specified dispatch timeout interval, depending on which condition is met first.

Note

The system response time might appear intermittent if the timeout interval is greater than 100 milliseconds and remote echoing is used. For lines with a reverse-Telnet connection, use a dispatch-timeout value less than 10 milliseconds.

Examples

The following example sets the dispatch timer to 80 milliseconds for virtual terminal line (vty) lines 0 through 4:

```
Router(config)# line vty 0 4
Router(config-line)# dispatch-timeout 80
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer-length</td>
<td>Specifies the maximum length of data streams forwarded on a line.</td>
</tr>
<tr>
<td>dispatch-character</td>
<td>Defines a character that causes a packet to be sent.</td>
</tr>
<tr>
<td>dispatch-machine</td>
<td>Specifies an identifier for a TCP packet dispatch state machine on a particular line.</td>
</tr>
<tr>
<td>state-machine</td>
<td>Specifies the transition criteria for the state of a particular state machine.</td>
</tr>
<tr>
<td>terminal dispatch-timeout</td>
<td>Sets the character dispatch timer for the current session.</td>
</tr>
</tbody>
</table>

**do**

To execute user EXEC or privileged EXEC commands from global configuration mode or other configuration modes or submodes, use the `do` command in any configuration mode.

```
do command
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Description</th>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>command</code></td>
<td>The user EXEC or privileged EXEC command to be executed.</td>
<td>A user EXEC or privileged EXEC command is not executed from a configuration mode.</td>
<td>All configuration modes</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12.2(8)T</td>
</tr>
</tbody>
</table>
Modification/Release
This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX
Support for this command was added for the Supervisor Engine 720.
12.2(17a)SX
This command was changed to support the copy command restriction.
12.2(17d)SXB
Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA
This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(3)T
This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines
Use this command to execute user EXEC or privileged EXEC commands (such as show, clear, and debug commands) while configuring your routing device. After the EXEC command is executed, the system will return to the configuration mode you were using.

Tip
This command can be useful for saving your configuration to the startup-config file without having to return to the user EXEC mode or privileged EXEC mode (do copy running-config startup-config) or for checking the status of a feature (using a do show command) while configuring the feature.

Caution
Do not enter the do command in user EXEC mode or privileged EXEC mode. Interruption of service might occur.

You cannot use the do command to execute the configure terminal command because entering the configure terminal command changes the user EXEC mode or privileged EXEC mode to the global configuration mode.

You cannot use the do command to execute copy or write commands in the global configuration or any other configuration mode or submode.

Examples
The following example shows how to enter the show interfaces serial privileged EXEC command from within global configuration mode:

Router(config)# do show interfaces serial 3/0
Serial3/0 is up, line protocol is up
  Hardware is MST-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of “show interface” counters never
  .
  .
  .

The following example shows how to enter the clear vpdn tunnel user EXEC or privileged EXEC command from within VPDN configuration mode:

Router(config-vpdn)# do clear vpdn tunnel
downward-compatible-config

To generate a configuration that is compatible with an earlier Cisco IOS release, use the `downward-compatible-config` command in global configuration mode. To disable this function, use the `no` form of this command.

```
downward-compatible-config version
no downward-compatible-config
```

### Syntax Description

<table>
<thead>
<tr>
<th><code>version</code></th>
<th>Cisco IOS release number, not earlier than Release 10.2.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Note</code></td>
<td>You must have a period (.) in the version number. For example, 12.4.</td>
</tr>
</tbody>
</table>

### Command Default

The configuration is not compatible with earlier Cisco IOS releases.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

In Cisco IOS Release 10.3, IP access lists changed format. Use the `downward-compatible-config` command to regenerate a configuration in a format prior to Release 10.3 if you will downgrade from your software version to version 10.2 or 10.3. The earliest `version` value this command accepts is 10.2.

When this command is configured, the router attempts to generate a configuration that is compatible with the specified version. Note that this command affects only IP access lists.

Under some circumstances, the software might not be able to generate a fully backward-compatible configuration. In such a case, the software issues a warning message.
Examples

The following example shows how to generate a configuration file compatible with Cisco IOS Release 10.2 access lists:

Router(config)# downward-compatible-config 10.2

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (extended)</td>
<td>Provides extended access lists that allow more detailed access lists.</td>
</tr>
<tr>
<td>access-list (standard)</td>
<td>Defines a standard XNS access list.</td>
</tr>
</tbody>
</table>

editing

To reenable Cisco IOS enhanced editing features for a particular line after they have been disabled, use the `editing` command in line configuration mode. To disable these features, use the `no` form of this command.

```
editing
do editing
```

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enhanced editing features are enabled by default. However, there may be situations in which you need to disable these features. The `no` form of this command disables these enhanced editing features, and the plain form of the command can be used to reenable these features.

The table below provides a description of the keys used to enter and edit commands when the editing features are enabled. Ctrl indicates the Control key, which must be pressed simultaneously with its associated letter key. Esc indicates the Escape key, which must be pressed first, followed by its associated letter key. A comma is used in the following table to indicate a key sequence (the comma key should not be pressed). Keys are not case sensitive. Many letters used for CLI navigation and editing were chosen to provide an easy way of remembering their functions. In the following table, characters are bolded in the “Function Summary” column to indicate the relation between the letter used and the function.
Table 23: Command Editing Keys and Functions

<table>
<thead>
<tr>
<th>Keys</th>
<th>Function Summary</th>
<th>Function Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
<td>Complete command</td>
<td>Completes a partial command name entry. When you enter a unique set of characters and press the Tab key, the system completes the command name. If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. To view the commands which match the set of characters you have entered, enter a question mark (?) immediately following the partial command (no space). The CLI will then list the commands that begin with that string.</td>
</tr>
<tr>
<td>Return (at the command line)</td>
<td>Execute</td>
<td>Executes the command.</td>
</tr>
<tr>
<td>Return (at the --More-- prompt)</td>
<td>Continue</td>
<td>Displays the next line of output.</td>
</tr>
<tr>
<td>Space Bar (at the --More-- prompt)</td>
<td>Continue</td>
<td>Displays the next screen of output. The amount of output you see will depend on the screen depth setting of your terminal.</td>
</tr>
<tr>
<td>Delete or Backspace</td>
<td>Backspace</td>
<td>Erases the character to the left of the cursor.</td>
</tr>
<tr>
<td>Left Arrow(^1) or Ctrl-B</td>
<td>Back character</td>
<td>Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.</td>
</tr>
<tr>
<td>Right Arrow(^1) or Ctrl-F</td>
<td>Forward character</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Esc, B</td>
<td>Back word</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc, F</td>
<td>Forward word</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Beginning of line</td>
<td>Moves the cursor to the beginning of the line.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>End of line</td>
<td>Moves the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td>Delete character</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Esc, D</td>
<td>Delete next word</td>
<td>Deletes from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Delete previous word</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Delete line forward</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-U or Ctrl-X</td>
<td>Delete line backward</td>
<td>Deletes all characters from the cursor back to the beginning of the command line.</td>
</tr>
<tr>
<td>Keys</td>
<td>Function Summary</td>
<td>Function Details</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ctrl-T</td>
<td>Transpose characters</td>
<td>Transposes the character to the left of the cursor with the character located at the cursor.</td>
</tr>
<tr>
<td>Ctrl-R or Ctrl-L</td>
<td>Redisplay line</td>
<td>Redisplays the system prompt and command line.</td>
</tr>
<tr>
<td>Ctrl-V or Esc, Q</td>
<td>Ignore editing</td>
<td>Inserts a code to indicate to the system that the keystroke immediately following should be treated as a command entry, not as an editing key.</td>
</tr>
<tr>
<td>Up Arrow1 or Ctrl-P</td>
<td>Previous command</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Down Arrow1 or Ctrl-N (next)</td>
<td>Next command</td>
<td>Returns to more recent commands in the history buffer (after recalling commands with the Up Arrow or Ctrl-P). Repeat the key sequence to recall successively more recent commands.</td>
</tr>
<tr>
<td>Ctrl-Y</td>
<td>Recall last deleted command</td>
<td>Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten items you have deleted or cut. Ctrl-Y can be used in conjunction with Esc Y.</td>
</tr>
<tr>
<td>Esc, Y</td>
<td>Recall next deleted command</td>
<td>Recalls the next entry in the delete buffer. The delete buffer contains the last ten items you have deleted. Press Ctrl-Y first to recall the most recent entry. Then press Esc Y up to nine times to recall the remaining entries in the buffer. If you bypass an entry, continue to press Esc Y to cycle back to it.</td>
</tr>
<tr>
<td>Esc, C</td>
<td>Capitalize word</td>
<td>Capitalizes the word from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Esc, U</td>
<td>Make word uppercase</td>
<td>Changes all letters from the cursor to the next space on the line appear in uppercase letters.</td>
</tr>
<tr>
<td>Esc, L</td>
<td>Make word lowercase</td>
<td>Changes the word to lowercase from the cursor to the end of the word.</td>
</tr>
</tbody>
</table>

1 The arrow keys function only with ANSI-compatible terminals.

**Examples**

In the following example, enhanced editing mode is disabled on line 3:

```
Router(config)# line 3
Router(config-line)# no editing
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal editing</td>
<td>Controls CLI enhanced editing feature for the current terminal session.</td>
</tr>
</tbody>
</table>
enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the enable command in either user EXEC, privileged EXEC, or diagnostic mode.

**enable [privilege-level] [view [view-name]]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>privilege-level</td>
<td>(Optional) Privilege level at which to log in.</td>
</tr>
<tr>
<td>view</td>
<td>(Optional) Enters into root view, which enables users to configure CLI views.</td>
</tr>
<tr>
<td>Note</td>
<td>This keyword is required if you want to configure a CLI view.</td>
</tr>
<tr>
<td>view-name</td>
<td>(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.</td>
</tr>
</tbody>
</table>

**Command Default**

Privilege-level 15 (privileged EXEC)

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>The <code>view</code> keyword and <code>view-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>The <code>view</code> keyword and <code>view-name</code> argument were integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(22)SB.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command became available on the ASR 1000 Series Routers, and became available in diagnostic mode for the first time.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, using the `enable` command without the `privilege-level` argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the `enable password` global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.
If an `enable` password has not been set, only enable mode can be accessed through the console connection. Security levels can be set by an administrator using the `enable password` and `privilege level` commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the `enable` command, the user will enter the default mode of privileged EXEC (level 15).

**Accessing a CLI View**

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the `enable view` command (without the `view-name` argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The `view-name` argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

**Examples**

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the `enable` command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the `disable` command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first
Password: 
00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
   configure Enter configuration mode
   enable Turn on privileged commands
   exit Exit from the EXEC
   show Show running system information
Router# show ?
   ip IP information
   parser Display parser information
   version System hardware and software status
Router# show ip ?
   access-lists List IP access lists
   accounting The active IP accounting database
   aliases IP alias table
   arp IP ARP table
```
The following example shows how to use the `enable view` command to switch from the root view to the CLI view “first”:

Router# `enable view`  
Router# 01:08:16:%PARSER-6-VIEW_SWITCH: successfully set to view 'root'.  
Router# ! Enable the show parser view command from the root view  
Router# `show parser view`  
Current view is 'root'  
! Enable the show parser view command from the root view to display all views  
Router# `show parser view all`  
Views Present in System:  
View Name:  first  
View Name:  second  
! Switch to the CLI view “first.”  
Router# `enable view first`  

Router# 01:08:09:%PARSER-6-VIEW_SWITCH: successfully set to view 'first'.  
! Enable the show parser view command from the CLI view “first.”  
Router# `show parser view`  
Current view is 'first'

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.</td>
</tr>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to various privilege levels.</td>
</tr>
<tr>
<td>privilege level (global)</td>
<td>Sets a privilege level for a command.</td>
</tr>
<tr>
<td>privilege level (line)</td>
<td>Sets a privilege level for a command for a specific line.</td>
</tr>
</tbody>
</table>
enable last-resort

To enable password parameters as the last resort without specifying the local enable password if no TACACS servers respond, use the **enable last-resort** command in global configuration mode. To disable the password parameters, use the **no** form of this command.

```
no enable last-resort {password|succeed}
no enable last-resort
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>password</strong></td>
<td>Enables password parameters by specifying the local enable password.</td>
</tr>
<tr>
<td><strong>succeed</strong></td>
<td>Enables password parameters without specifying the local enable password.</td>
</tr>
</tbody>
</table>

**Command Default**

The password parameters for the router are not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(M)</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(M).</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable password parameters as the last resort without specifying the local enable password if no TACACS servers respond:

```
Router> enable
Router# configure terminal
Router(config)# enable last-resort succeed
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show tacacs</strong></td>
<td>Displays statistics for a TACACS+ server.</td>
<td></td>
</tr>
</tbody>
</table>

**end**

To end the current configuration session and return to privileged EXEC mode, use the **end** command in global configuration mode.

```
end
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This command has no arguments or keywords.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
This command will bring you back to privileged EXEC mode regardless of what configuration mode or configuration submode you are in.

This global configuration command can be used in any configuration mode.

Use this command when you are done configuring the system and you want to return to EXEC mode to perform verification steps.

In the following example, the `end` command is used to exit from ALPS ASCU configuration mode and return to privileged EXEC mode. A `show` command is used in privileged EXEC mode to verify the configuration.

```
Router# configure terminal
Router(config)# interface serial 1:1
Router(config-if)# alps ascu 4B
Router(config-alps-ascu)# end
Router# show interface serial 1:1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit (global)</td>
<td>Exits from the current configuration mode.</td>
</tr>
</tbody>
</table>

### environment-monitor shutdown temperature

To enable monitoring of the environment sensors, use the `environment-monitor shutdown temperature` command in global configuration mode. To disable monitoring of the environment sensors, use the `no` form of this command.

```
environment-monitor shutdown temperature [rommon|powerdown]
no environment-monitor shutdown temperature [rommon|powerdown]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rommon</td>
<td>(Optional) Places the supervisor engine in ROMMON when a major active alarm is identified.</td>
</tr>
<tr>
<td>powerdown</td>
<td>(Optional) Powers down the supervisor engine when a new active major alarm is identified.</td>
</tr>
</tbody>
</table>

#### Command Default

By default, `rommon` is enabled.

#### Command Modes

Global configuration


**environment temperature-controlled**

To enable the ambient temperature control, use the `environment temperature-controlled` command in global configuration mode. To disable the ambient temperature control, use the `no` form of this command.

```
Router(config)#
environment-monitor shutdown temperature rommon
Router(config)#
```

This example shows how to power down the supervisor engine when a major active alarm occurs:

```
Router(config)#
environment-monitor shutdown temperature powerdown
Router(config)#
```

This command does not affect temperature monitoring and alarm thresholds; it only affects whether a module may be powered on. The software does not validate the inlet temperature.

If you enter the `no` form of this command and the cooling capacity is reduced below the module cooling requirement, a syslog warning (and SNMP alarm) is generated. This module status does not change, and an environmental alarm is not raised when you enter the `no` form of this command.
**Examples**

This example shows how to enable the ambient temperature control:

```plaintext
Router(config)#
environment temperature-controlled
Router(config)#
```

This example shows how to disable the ambient temperature control:

```plaintext
Router(config)#
no environment temperature-controlled
Router(config)#
```

## erase

To erase a file system or all files available on a file system, use the `erase` command in privileged EXEC or diagnostic mode.

```
erase { /all nvram:/no-squeeze-reserve-space filesystem:filesystem : [startup-config] }
erase { /all nvram:/filesystem:[startup-config] }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/all</td>
<td>Erases all files in the specified file system.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Erases all files in the NVRAM.</td>
</tr>
<tr>
<td>filesystem:</td>
<td>File system name, followed by a colon. For example, flash: or nvram:.</td>
</tr>
<tr>
<td>/no-squeeze-reserve-space</td>
<td>Disables the squeeze operation to conserve memory and makes the erase command compatible with older file systems.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Erases the contents of the configuration memory.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#) Diagnostic (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(11)T</td>
<td>This command was modified. The /no-squeeze-reserve-space keyword was added.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was modified. Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Modification

This command was modified. The command was introduced in diagnostic mode on the Cisco ASR 1000 Series Routers, and the /all keyword was added.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The file-system : argument was added.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

The `erase nvram`: command replaces the `write erase` command and the `erase startup-config` command.

When you use the `erase` command to erase a file system, you cannot recover the files in the file system.

Caution

The `word help` feature is disabled for the `erase` command. You must enter the complete command name to enable the command. The parser does not complete the command name if you enter partial syntax of the command and press the Tab key. For more information on the word help feature, refer to the Using the Cisco IOS Command-Line Interface feature guide.

The `erase` command can be used on Class B and Class C flash file systems only.

Class A flash file systems cannot be erased. You can delete individual files using the `delete` command and then reclaim the space using the `squeeze` command. You can use the `format` command to format the flash file system. The `format` command when used on ATA disk clears the File Allocation Table (FAT) and root directory entries only. The data is not erased.

The `erase nvram`: command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in flash memory, the specified file will be marked “deleted.”

The `erase /all nvram`: command erases all files on NVRAM, including private NVRAM.

The `/no-squeeze-reserve-space` keyword is available on systems with small amounts of flash memory in order to conserve memory. When a squeeze operation is performed, the last two erase sectors are permanently reserved for the squeeze logs and squeeze buffer. The `/no-squeeze-reserve-space` keyword prevents the reservation of space that guarantees the ability to run the squeeze command. Disabling the squeeze operation keeps these memory sectors free. If any sectors using squeeze data are detected, they will be erased when the `/no-squeeze-reserve-space` keyword is used. The `/no-squeeze-reserve-space` keyword increases the available amount of usable flash space, but you may not be able to run the `squeeze` command. This is typically fine if the file system (such as flash) is used to store a single, large file. For example, an IOS image.

On Class C flash file systems, space is dynamically reclaimed when you use the `delete` command. You can also use either the `format` or `erase` command to reinitialize a Class C flash file system.

Note

Use the context-sensitive help to determine which file systems can be used for the `erase` command. The output will vary based on the platform.

Examples

The following example shows how to erase the NVRAM, including the startup configuration located there:

`Router# erase nvram:`

The following example shows how to erase all of partition 2 in internal flash memory:
Router# erase flash:2

System flash directory, partition 2:
File Length Name/status
1 1711088 dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]
Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased

The following example shows how to erase flash memory when flash is partitioned, but no partition is specified in the command:

Router# erase flash:
System flash partition information:
Partition Size Used Free Bank-Size State Copy-Mode
1 4096K 2048K 2048K 2048K Read Only RXBOOT-FLH
2 4096K 2048K 2048K 2048K Read/Write Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]

The system will prompt only if there are two or more read/write partitions. If the partition entered is not valid or is the read-only partition, the process terminates. You can enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (?
umber) for directory display of a particular partition. The default is the first read/write partition.

System flash directory, partition 2:
File Length Name/status
1 3459720 master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Erase flash device, partition 2? [confirm] <Return>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file on a flash memory device.</td>
</tr>
<tr>
<td>more nvram:startup-config</td>
<td>Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
</tr>
<tr>
<td>squeeze</td>
<td>Removes all deleted files from the flash file system and recovers the memory space used by deleted files.</td>
</tr>
<tr>
<td>undelete</td>
<td>Recovers a file marked “deleted” on a Class A or Class B flash file system.</td>
</tr>
<tr>
<td>write erase</td>
<td>The write erase command is replaced by the erase nvram: command. See the description of the erase command for more information.</td>
</tr>
</tbody>
</table>
erase bootflash

The `erase bootflash` command has identical functions. See the description of the `erase` command in this chapter for more information.

errdisable detect cause

To enable error-disable detection, use the `errdisable detect cause` command in global configuration mode. To disable error-disable detection, use the `no` form of this command.

```
errdisable detect cause {all|bpdu-guard|dtp-flap|l2pt-guard|link-flap|packet-buffer-error|pagp-flap|root-guard|udld}
no errdisable detect cause {all|bpdu-guard|dtp-flap|l2pt-guard|link-flap|pagp-flap|root-guard|udld}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Specifies error-disable detection for all error-disable causes.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bpdu-guard</td>
<td>Specifies detection for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.</td>
</tr>
<tr>
<td></td>
<td>dtp-flap</td>
<td>Specifies detection for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.</td>
</tr>
<tr>
<td></td>
<td>link-flap</td>
<td>Specifies detection for the link flap error-disable cause.</td>
</tr>
<tr>
<td></td>
<td>packet-buffer-error</td>
<td>Causes the packet buffer error to error-disable the affected port.</td>
</tr>
<tr>
<td></td>
<td>pagp-flap</td>
<td>Specifies detection for the Port Aggregation Protocol (PAgP)-flap error-disable cause.</td>
</tr>
<tr>
<td></td>
<td>root-guard</td>
<td>Specifies detection for the root-guard error-disable cause.</td>
</tr>
<tr>
<td></td>
<td>udld</td>
<td>Specifies detection for the Unidirectional Link Detection (UDLD) error-disable cause.</td>
</tr>
</tbody>
</table>

Command Default

Error-disable detection is enabled for all causes.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was modified. Support was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was modified. The <code>packet-buffer-error</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Note

Entering the `no errdisable detect cause packet-buffer-error` command allows you to detect the fault that triggers a power cycle of the affected module.

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, root-guard, udld) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similar to the link-down state).

You must enter the `shutdown` and then the `no shutdown` commands to recover an interface manually from the error-disable state.

Examples

The following example shows how to enable error-disable detection for the Layer 2 protocol-tunnel guard error-disable cause:

```
Router(config)#
errdisable detect cause l2ptguard
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show errdisable detect</td>
<td>Displays the error-disable detection status.</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays the interface status or a list of interfaces in an error-disable state on LAN ports only.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>

errdisable recovery

To configure recovery mechanism variables, use the `errdisable recovery` command in global configuration mode. To return to the default state, use the `no` form of this command.

```
errdisable recovery {cause [arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap | psecure-violation | security-violation | root-guard | udld | unicast-flood] [interval seconds]}
no errdisable recovery {cause [arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap | psecure-violation | security-violation | root-guard | udld | unicast-flood] [interval seconds]}
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cause</td>
<td>Enables error-disable recovery from a specific cause.</td>
</tr>
<tr>
<td>all</td>
<td>Enables the recovery timers for all error-disable causes.</td>
</tr>
<tr>
<td>arp-inspection</td>
<td>Enables error-disable recovery from an Address Resolution Protocol (ARP) inspection cause.</td>
</tr>
<tr>
<td>bpduguard</td>
<td>Enables the recovery timer for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.</td>
</tr>
</tbody>
</table>
Enable the recovery timer for the channel-misconfig error-disable cause.

Enable the recovery timer for the Dynamic Host Configuration Protocol (DHCP)-rate-limit error-disable cause.

Enable the recovery timer for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.

Enable the recovery timer for the Gigabit Interface Converter (GBIC)-invalid error-disable cause.

Enable the recovery timer for the Layer 2 Protocol Tunneling (L2PT) error-disable cause.

Enable the recovery timer for the link-flap error-disable cause.

Enable the recovery timer for the Port Aggregation Protocol (PAgP)-flap error-disable cause.

Enable the recovery timer for the psecure-violation error-disable cause.

Enable the automatic recovery of ports that were disabled because of 802.1X security violations.

Enable the recovery timer for the root-guard error-disable cause.

Enable the recovery timer for the Unidirectional Link Detection (UDLD) error-disable cause.

Enable the recovery timer for the unicast-flood error-disable cause.

Specifies the time, in seconds, to recover from a specified error-disable cause. The range is from 30 to 86400. The default interval is 300.

<table>
<thead>
<tr>
<th>command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-misconfig</td>
<td>Enables the recovery timer for the channel-misconfig error-disable cause.</td>
</tr>
<tr>
<td>dhcp-rate-limit</td>
<td>Enables the recovery timer for the Dynamic Host Configuration Protocol (DHCP) RATE-LIMIT error-disable cause.</td>
</tr>
<tr>
<td>dtp-flap</td>
<td>Enables the recovery timer for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.</td>
</tr>
<tr>
<td>gbic-invalid</td>
<td>Enables the recovery timer for the Gigabit Interface Converter (GBIC)-invalid error-disable cause.</td>
</tr>
<tr>
<td>l2ptguard</td>
<td>Enables the recovery timer for the Layer 2 Protocol Tunneling (L2PT) error-disable cause.</td>
</tr>
<tr>
<td>link-flap</td>
<td>Enables the recovery timer for the link-flap error-disable cause.</td>
</tr>
<tr>
<td>pagg-flap</td>
<td>Enables the recovery timer for the Port Aggregation Protocol (PAgP)-flap error-disable cause.</td>
</tr>
<tr>
<td>psecure-violation</td>
<td>Enables the recovery timer for the psecure-violation error-disable cause.</td>
</tr>
<tr>
<td>security-violation</td>
<td>Enables the automatic recovery of ports that were disabled because of 802.1X security violations.</td>
</tr>
<tr>
<td>rootguard</td>
<td>Enables the recovery timer for the root-guard error-disable cause.</td>
</tr>
<tr>
<td>udlld</td>
<td>Enables the recovery timer for the Unidirectional Link Detection (UDLD) error-disable cause.</td>
</tr>
<tr>
<td>unicast-flood</td>
<td>Enables the recovery timer for the unicast-flood error-disable cause.</td>
</tr>
<tr>
<td>interval seconds</td>
<td>Specifies the time, in seconds, to recover from a specified error-disable cause. The range is from 30 to 86400. The default interval is 300.</td>
</tr>
</tbody>
</table>

**Command Default**

The recovery mechanisms are disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was modified. This command was implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was modified. This command was implemented on the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was modified. The arp-inspection keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

A cause (bpduguard, channel-misconfig, dhcp-rate-limit, dtp-flap, l2ptguard, link-flap, pagp-flap, psecure-violation, security-violation, rootguard, udlld, or unicast-flood) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disable state until a shutdown and no shutdown occur. If you enable recovery for a cause, the interface is brought out of the error-disable state and allowed to retry operation once all the causes have timed out.

You must enter the `shutdown` command and then the `no shutdown` command to manually recover an interface from the error-disable state.

Note

A separate line is required each time you want to enter the `errdisable recovery cause` command to add a new reason for recovery; each new reason does not get appended to the original single line. This means you must enter each new reason separately.

Examples

This example shows how to enable the recovery timer for the BPDU-guard error-disable cause:

```
Router(config)#
errdisable recovery cause bpduguard
```

This example shows how to set the recovery timer to 300 seconds:

```
Router(config)#
errdisable recovery interval 300
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show errdisable recovery</td>
<td>Displays the information about the error-disable recovery timer.</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>

escape-character

To define a system escape character, use the `escape-character` command in line configuration mode. To set the escape character to Break, use the `no` `default` form of this command.

```
escape-character {break|char|default|none|soft}
no escape-character [soft]
default escape-character [soft]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>break</td>
<td>Sets the escape character to Break. Note that the Break key should not be used as an escape character on a console terminal.</td>
</tr>
<tr>
<td>char</td>
<td>Character (for example, !) or its ASCII decimal representation (integer in the range of 0 to 255) to be used as the escape character.</td>
</tr>
</tbody>
</table>
**escape-character**

<table>
<thead>
<tr>
<th>default</th>
<th>Sets the escape key sequence to the default of Ctrl-^, X.</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Disables escape entirely.</td>
</tr>
<tr>
<td>soft</td>
<td>Sets an escape character that will wait until pending input is processed before it executes.</td>
</tr>
</tbody>
</table>

**Command Default**

The default escape key sequence is Ctrl-Shift-6 (Ctrl-\^) or Ctrl-Shift-6, X (\^X). The X is generally only required for modem connections.

The **default escape-character** command sets the escape character to Break (the default setting for Break is Ctrl-C).

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3</td>
<td>The <strong>soft</strong> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

See the "ASCII Character Set and Hexadecimal Values" appendix for a list of ASCII characters.

The escape character (or key sequence) suspends any actively running processes and returns you to privileged EXEC mode or, if a menu is being used, to the system menu interface. The escape character is used for interrupting or aborting a process started by previously executed command. Examples of processes from which you can escape include Domain-Name lookup, ping, trace, and Telnet sessions initiated from the device to which you are connected.

To view the current setting of the escape sequence for a line, use the **show line** command followed by the specific line identifier (for example, show line 0, or show line console). The default escape sequence for a line is often displayed as \^X. The first caret symbol represents the Control (Ctrl) key, the second caret symbol is literal (Shift-6), and the X is literal (for most systems, the X is not required).

To set the escape key for the active terminal line session, use the **terminal escape-character** command.

The Break key cannot be used as an escape character on a console terminal because the Cisco IOS software interprets Break as an instruction to halt the system. Depending upon the configuration register setting, break commands issued from the console line either will be ignored or cause the server to shut down.

To send an escape sequence over a Telnet connection, press **Ctrl-Shift-6** twice.

The escape-character **soft** form of this command defines a character or character sequence that will cause the system to wait until pending input is processed before suspending the current session. This option allows you to program a key sequence to perform multiple actions, such as using the F1 key to execute a command, then execute the escape function after the first command is executed.

The following restrictions apply when using the **soft** keyword:

- The length of the logout sequence must be 14 characters or fewer.
- The soft escape character cannot be the same as the generic Cisco escape character, Break, or the characters b, d, n, or s.
- The soft escape character should be an ASCII value from 1 to 127. Do not use the number 30.
The following examples set the escape character for the console line to the keyboard entry Ctrl-P, which is represented by the ASCII decimal value of 16:

Router(config)# line console
Router(config-line)# escape-character 16

The following example sets the escape character for line 1 to !, which is represented in the configuration file as the ASCII number 33:

Router(config)# line 1
Router(config-line)# escape-character !
Router(config-line)# end
Router# show running-config
Building configuration...

line 1
  autoselect during-login
  autoselect ppp
  modem InOut
  transport preferred none
  transport output telnet
  escape-character 33

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show line</td>
<td>Displays information about the specified line connection, or all the lines.</td>
</tr>
<tr>
<td>terminal escape-character</td>
<td>Sets the escape character for the current terminal line for the current session.</td>
</tr>
</tbody>
</table>

### exec

To allow an EXEC process on a line, use the `exec` command in line configuration mode. To turn off the EXEC process for the specified line, use the `no` form of this command.

```
exec
no exec
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

The EXEC processes is enabled on all lines.

### Command Modes

Line configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you want to allow only an outgoing connection on a line, use the `no exec` command.
The **no exec** command allows you to disable the EXEC process for connections which may attempt to send unsolicited data to the router. (For example, the control port of a rack of modems attached to an auxiliary port of router.) When certain types of data are sent to a line connection, an EXEC process can start, which makes the line unavailable.

When a user tries to Telnet to a line with the EXEC process disabled, the user will get no response when attempting to log on.

### Examples

The following example disables the EXEC process on line 7.

```
Router(config)# line 7
Router(config-line)# no exec
```

### exec-banner

To reenable the display of EXEC and message-of-the-day (MOTD) banners on the specified line or lines, use the **exec-banner** command in line configuration mode. To suppress the banners on the specified line or lines, use the **no** form of this command.

**exec-banner**

**no exec-banner**

### Syntax Description

This command has no arguments or keywords.

### Command Default

Enabled on all lines

### Command Modes

Line configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command determines whether the router will display the EXEC banner and the message-of-the-day (MOTD) banner when an EXEC session is created. These banners are defined with the **banner exec** and **banner motd** global configuration commands. By default, these banner are enabled on all lines. Disable the EXEC and MOTD banners using the **no exec-banner** command.

This command has no effect on the incoming banner, which is controlled by the **banner incoming** command.

The MOTD banners can also be disabled by the **no motd-banner** line configuration command, which disables MOTD banners on a line. If the **no exec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner** command is enabled or disabled. The table below summarizes the effects of the **exec-banner** command and the **motd-banner** command.
Table 24: Banners Displayed Based On exec-banner and motd-banner Combinations

<table>
<thead>
<tr>
<th></th>
<th>exec-banner (default)</th>
<th>no exec-banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>motd-banner (default)</td>
<td>MOTD banner</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>EXEC banner</td>
<td>None</td>
</tr>
<tr>
<td>no motd-banner</td>
<td>EXEC banner</td>
<td>None</td>
</tr>
</tbody>
</table>

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **no exec-banner** command or **no motd-banner** command is configured. The table below summarizes the effects of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

Table 25: Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines

<table>
<thead>
<tr>
<th></th>
<th>exec-banner (default)</th>
<th>no exec-banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>motd-banner (default)</td>
<td>MOTD banner</td>
<td>Incoming banner</td>
</tr>
<tr>
<td></td>
<td>Incoming banner</td>
<td>Incoming banner</td>
</tr>
<tr>
<td>no motd-banner</td>
<td>Incoming banner</td>
<td>Incoming banner</td>
</tr>
</tbody>
</table>

**Examples**

The following example suppresses the EXEC and MOTD banners on virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)# no exec-banner
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>banner exec</strong></td>
<td>Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.</td>
</tr>
<tr>
<td><strong>banner incoming</strong></td>
<td>Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.</td>
</tr>
<tr>
<td><strong>banner motd</strong></td>
<td>Defines and enables a customized message-of-the-day banner.</td>
</tr>
<tr>
<td><strong>motd-banner</strong></td>
<td>Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.</td>
</tr>
</tbody>
</table>

**exec-character-bits**

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

```
exec-character-bits {7|8}
no exec-character-bits
```
Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Selects the 7-bit character set. This is the default.</td>
</tr>
<tr>
<td>8</td>
<td>Selects the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on.</td>
</tr>
</tbody>
</table>

Command Default

7-bit ASCII character set

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. If a user on a terminal that is sending parity enters the `help` command, an “unrecognized command” message appears because the system is reading all 8 bits, and the eighth bit is not needed for the `help` command.

Note

If you are using the `autoselect` function, set the activation character to the default (Return) and the value for `exec-character-bits` to 7. If you change these defaults, the application will not recognize the activation request.

Examples

The following example enables full 8-bit international character sets, except for the console, which is an ASCII terminal. It illustrates use of the `default-value exec-character-bits` global configuration command and the `exec-character-bits` line configuration command.

```
Router(config)# default-value exec-character-bits 8
Router(config)# line 0
Router(config-line)# exec-character-bits 7
```
exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the exec-timeout command in line configuration mode. To remove the timeout definition, use the no form of this command.

```
exec-timeout minutes [seconds]
no exec-timeout
```

**Syntax Description**
- `minutes`: Integer that specifies the number of minutes. The default is 10 minutes.
- `seconds`: (Optional) Additional time intervals in seconds.

**Command Default**
- 10 minutes

**Command Modes**
- Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)SY2</td>
<td>The <strong>no</strong> form of the command updated to configure an exec-timeout of 0 0 on the device.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

To specify no timeout, enter the **no** form of this command.

**Examples**

The following example sets a time interval of 2 minutes, 30 seconds:

```
Router(config)# line console 0
Router(config-line)# exec-timeout 2 30
```

The following example sets a time interval of 10 seconds:

```
Router(config)# line console 0
Router(config-line)# exec-timeout 0 10
```

**execute-on**

To execute commands on a line card, use the execute-on command in privileged EXEC mode.

```
execute-on {slot slot-number|all|master} command
```
Syntax Description

<table>
<thead>
<tr>
<th><strong>slot slot-number</strong></th>
<th>Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Cisco 12012 router: 0 to 11</td>
</tr>
<tr>
<td></td>
<td>• Cisco 12008 access server: 0 to 7</td>
</tr>
<tr>
<td></td>
<td>• Cisco AS5800 access server: 0 to 13</td>
</tr>
</tbody>
</table>

| **all**             | Executes the command on all line cards.         |
| **master**          | (AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only. |
| **command**         | Cisco IOS command to remotely execute on the line card. |

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 GS</td>
<td>This command was introduced to support Cisco 12000 series Gigabit Switch Routers.</td>
</tr>
<tr>
<td>11.3(2)AA</td>
<td>This command was implemented in images for the Cisco AS5800 series.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE. Pipe &quot;</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to execute a command on one or all line cards to monitor and maintain information on one or more line cards (for example, a line card in a specified slot on a dial shelf). This allows you to issue commands remotely; that is, to issue commands without needing to log in to the line card directly. The **all** form of the command allows you to issue commands to all the line cards without having to log in to each in turn.

Though this command does not have a **no** form, note that it is possible to use the **no** form of the remotely executed commands used in this command.

Tip

This command is useful when used with **show EXEC** commands (such as **show version**), because you can verify and troubleshoot the features found only on a specific line card. Please note, however, that because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Cisco 12000 GSR Guidelines and Restrictions

You can use the **execute-on** privileged EXEC command only from Cisco IOS software running on the GRP card.
Though you can use the `attach` privileged EXEC command to execute commands on a specific line card, using the `execute-on slot` command saves you some steps. For example, first you must use the `attach` command to connect to the Cisco IOS software running on the line card. Next you must issue the command. Finally you must disconnect from the line card to return to the Cisco IOS software running on the GRP card. With the `execute-on slot` command, you can perform three steps with one command. In addition, the `execute-on all` command allows you to perform the same command on all line cards simultaneously.

### Cisco c7600 Sup Guidelines and Restrictions

Beginning with the 12.2(33)SRE Cisco IOS release, all pipe "|" options can now be used with show option in the execute-on command on SUP and SAMI consoles.

### Cisco AS5800 Guidelines and Restrictions

The purpose of the command is to conveniently enable certain commands to be remotely executed on the dial shelf cards from the router without connecting to each line card. This is the recommended procedure, because it avoids the possibility of adversely affecting a good configuration of a line card in the process. The `execute-on` command does not give access to every Cisco IOS command available on the Cisco AS5800 access server. In general, the purpose of the `execute-on` command is to provide access to statistical reports from line cards without directly connecting to the dial shelf line cards.

**Caution**

Do not use this command to change configurations on dial shelf cards, because such changes will not be reflected in the router shelf.

Using this command makes it possible to accumulate inputs for inclusion in the `show tech-support` command.

The `master` form of the command can run a designated command remotely on the router from the DSC card. However, using the console on the DSC is not recommended. It is used for technical support troubleshooting only.

The `show tech-support` command for each dial shelf card is bundled into the router shelf’s `show tech-support` command via the `execute-on` facility.

The `execute-on` command also support interactive commands such as the following:

```plaintext
router: execute-on slave slot

slot
  ping
```

The `execute-on` command has the same limitations and restrictions as a `vty telnet` client has; that is, it cannot reload DSC using the following command:

```plaintext
router: execute-on slave slot

slot
  reload
```

You can use the `execute-on` command to enable remote execution of the commands included in the following partial list:

- `debug dsc clock`
• show context
• show diag
• show environment
• show dsc clock
• show dsi
• show dsip
• show tech-support

Examples

In the following example, the user executes the **show controllers** command on the line card in slot 4 of a Cisco 12000 series GSR:

Router# execute-on slot 4 show controllers
--------- Line Card (Slot 4) ----------
Interface POS0
Hardware is BFLC POS
lcpos_instance struct 6033A6E0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000400
SUNI rsop intr status 00
CRC16 enabled, HDLC enc, int clock
no loop
Interface POS1
Hardware is BFLC POS
lcpos_instance struct 6033CEC0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000600
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop
Interface POS2
Hardware is BFLC POS
lcpos_instance struct 6033F6A0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000800
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop
Interface POS3
Hardware is BFLC POS
lcpos_instance struct 60341E80
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000A00
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, ext clock
no loop
Router#

In the following example, the user executes the **show version** command on the line card in slot 2 and 3 of a Cisco c7600 Sup series device:
Example for c7600 SUP -
Router#execute-on 2 3 show

| Command to be executed |
| Output modifiers |

Router#execute-on 2 3 show version

| ? |
| append Append redirected output to URL (URLs supporting append operation only) |
| begin Begin with the line that matches |
| exclude Exclude lines that match |
| format Format the output using the specified spec file |
| include Include lines that match |
| redirect Redirect output to URL |
| section Filter a section of output |
| tee Copy output to URL |

Router#execute-on 2 3 execute-on 4 show version

| ? |
| append Append redirected output to URL (URLs supporting append operation only) |
| begin Begin with the line that matches |
| exclude Exclude lines that match |
| format Format the output using the specified spec file |
| include Include lines that match |
| redirect Redirect output to URL |
| section Filter a section of output |
| tee Copy output to URL |

In the following example, the user executes the **show** command on the line card in slot 4 of a Cisco c7600 SAMI series device:

Router#execute-on 4 show

| ? |
| append Append redirected output to URL (URLs supporting append operation only) |
| begin Begin with the line that matches |
| exclude Exclude lines that match |
| format Format the output using the specified spec file |
| include Include lines that match |
| redirect Redirect output to URL |
| section Filter a section of output |
| tee Copy output to URL |
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach</td>
<td>Connects you to a specific line card for the purpose of executing commands using the Cisco IOS software image on that line card.</td>
</tr>
</tbody>
</table>

**exit (EXEC)**

To close an active terminal session by logging off the router, use the `exit` command in EXEC mode.

```
exit
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `exit` command in EXEC mode to exit the active session (log off the device). This command can be used in any EXEC mode (such as User EXEC mode or Privileged EXEC mode) to exit from the EXEC process.

**Examples**

In the following example, the `exit` (global) command is used to move from global configuration mode to privileged EXEC mode, the `disable` command is used to move from privileged EXEC mode to user EXEC mode, and the `exit` (EXEC) command is used to log off (exit the active session):

```
Router(config)# exit
Router# disable
Router> exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disconnect</td>
<td>Disconnects a line.</td>
</tr>
<tr>
<td>end</td>
<td>Ends your configuration session by exiting to EXEC mode.</td>
</tr>
<tr>
<td>exit (global)</td>
<td>Exits from the current configuration mode to the next highest configuration mode.</td>
</tr>
<tr>
<td>logout</td>
<td>Closes your connection to the device (equivalent to the <code>exit</code> command).</td>
</tr>
</tbody>
</table>

**exit (global)**

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the `exit` command in any configuration mode.
exit

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
All configuration modes

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The exit command is used in the Cisco IOS CLI to exit from the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the exit command in global configuration mode to return to privileged EXEC mode. Use the exit command in interface, line, or router configuration mode to return to global configuration mode. Use the exit command in subinterface configuration mode to return to interface configuration mode. At the highest level, EXEC mode, the exit command will exit the EXEC mode and disconnect from the router interface (see the description of the exit (EXEC) command for details).

Examples
The following example shows how to exit from the subinterface configuration mode and to return to the interface configuration mode:

```
Router(config-subif)# exit
Router(config-if)#
```

The following example displays an exit from the interface configuration mode to return to the global configuration mode:

```
Router(config-if)# exit
Router(config)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disconnect</td>
<td>Disconnects a line.</td>
</tr>
<tr>
<td>end</td>
<td>Ends your configuration session by exiting to privileged EXEC mode.</td>
</tr>
<tr>
<td>exit (EXEC)</td>
<td>Closes the active terminal session by logging off the router.</td>
</tr>
</tbody>
</table>
F through K

- F through K, on page 198
file privilege

To configure a new file privilege level for users use the `file privilege` command in global configuration mode. To reset the file privilege level of the files to the default and remove the file privilege level configuration from the running configuration file, use the `no` form of this command.

```
file privilege level level
no file privilege level level
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level</code></td>
<td>Specifies the file privilege level for the files. The level argument must be a number from 0 to 15. Users with privilege level equal to greater than the file privilege level can access the files under the file system.</td>
</tr>
</tbody>
</table>

**Command Default**

By default the privilege level is set to 15.

**Command Modes**

Global configuration (config#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example, shows how to set the file privilege level to 3 and verify the change using the `show running-config` command.

```
Device(config)# file privilege ?
<0-15> Privilege level

Device(config)# file privilege 3
Device(config)# end

Device# show running-config | i file priv
file privilege 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>privilege level</code></td>
<td>Sets the default privilege level for a line.</td>
</tr>
</tbody>
</table>

file prompt

To specify the level of prompting, use the `file prompt` command in global configuration mode.

```
file prompt prompt [{alert|noisy|quiet}]
```
file prompt only for destructive file operations. This is the default.

**noisy** (Optional) Confirms all file operation parameters.

**quiet** (Optional) Seldom prompts for file operations.

**Command Default**

- alert

**Command Modes**

- Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to change the amount of confirmation needed for different file operations. This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

**Examples**

The following example configures confirmation prompting for all file operations:

```
Router(config)# file prompt noisy
```

---

**file verify auto**

To enable automatic image verification, use the `file verify auto` command in global configuration mode. To disable automatic image verification, use the `no` form of this command.

```
file verify auto
no file verify auto
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Image verification is not automatically applied to all images that are copied or reloaded onto a router.

**Command Modes**

- Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support was added for the Supervisor Engine 2.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

Image verification is accomplished by verifying the compressed Cisco IOS image checksum.

Image verification allows users to automatically verify the integrity of all Cisco IOS images. Thus, users can be sure that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

The **file verify auto** command enables image verification globally; that is, all images that are to be copied (via the **copy** command) or reloaded (via the **reload** command) are automatically verified. Although both the **copy** and **reload** commands have a `/verify` keyword that enables image verification, you must issue the keyword each time you want to copy or reload an image. The **file verify auto** command enables image verification by default so you no longer have to specify image verification multiple times.

If you have enabled image verification by default but prefer to disable verification for a specific image copy or reload, the `/noverify` keyword along with either the **copy** or the **reload** command will override the **file verify auto** command.

### Examples

The following example shows how to enable automatic image verification:

```
Router(config)# file verify auto
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>copy</strong></td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td><strong>copy/noverify</strong></td>
<td>Disables the automatic image verification for the current copy operation.</td>
</tr>
<tr>
<td><strong>reload</strong></td>
<td>Reloads the operating system.</td>
</tr>
<tr>
<td><strong>verify</strong></td>
<td>Verifies the checksum of a file on a Flash memory file system or computes an MD5 signature for a file.</td>
</tr>
</tbody>
</table>

### format

To format a Class A, Class B, or Class C flash memory file system, use the **format** command in privileged EXEC or diagnostic mode.

**Class B and Class C Flash File Systems**

```
format filesystem1:
```

**Class A Flash File System**

```
format [spare spare-number] filesystem1: [[filesystem2:][monlib-filename]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>spare</strong></td>
<td>(Optional) Reserves spare sectors as specified by the <strong>spare-number</strong> argument when you format flash memory.</td>
</tr>
<tr>
<td>spare-number</td>
<td>(Optional) Number of the spare sectors to reserve in formatted flash memory. Valid values are from 0 to 16. The default value is 0.</td>
</tr>
<tr>
<td>filesystem1 :</td>
<td>Flash memory to format, followed by a colon. Valid values for use with the Cisco 7600 series router are <code>disk0; disk1; bootflash; slot0; sup-slot0; and sup-bootflash</code>; see the “Usage Guidelines” section for additional information. Valid values for use with the ASR 1000 Series Routers are <code>bootflash; harddisk; stby-harddisk; obfl; and usb[0 1]</code>.</td>
</tr>
<tr>
<td>filesystem2 :</td>
<td>(Optional) File system containing the monlib file to use for formatting the argument <code>filesystem1</code> followed by a colon.</td>
</tr>
<tr>
<td>monlib-filename</td>
<td>(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the <code>filesystem1</code> argument. The default monlib file is the one bundled with the system software. Dual Route Switch Processors (RSP) High System Availability (HSA) Functionality When this command is used with Dual RSPs and you do not specify the <code>monlib-filename</code> argument, the system takes the ROM monitor library file from the slave image bundle. If you specify the <code>monlib-filename</code> argument, the system assumes that the files reside on the slave devices.</td>
</tr>
</tbody>
</table>

**Command Default**

`spare-number : 0monlib-filename`: The monlib file bundled with the system software

**Command Modes**

Privileged EXEC (#)
Diagnostic (diag)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>Support for Class B flash (USB flash and USB eToken) file systems was added as part of the USB Storage feature.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Cisco IOS XE Release 2.1 This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced:

- This command was introduced in diagnostic mode for the first time. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers.
- The `harddisk; obfl; stby-harddisk; stby-usb[0-1]; and usb[0-1]: filesystem1 :` options were introduced.
**Release** | **Modification**
---|---
12.2YST | This command was integrated into Cisco IOS Release 12.2YST.

**Usage Guidelines**

Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the flash memory card can still be used. Otherwise, you must reformat the flash card after some of the sectors fail.

Use this command to format Class A, B, or C flash memory file systems. The Cisco 7600 series router supports only Class A and Class C flash file systems.

In some cases, you might need to insert a new Personal Computer Memory Card Industry Association (PCMCIA) flash memory or flash PC card and load images or backup configuration files onto it. Before you can use a new flash memory or flash PC card, you must format it.

Sectors in flash memory or flash PC cards can fail. Reserve certain flash memory or flash PC sectors as “spares” by using the optional spare-number argument on the `format` command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the flash memory or flash PC card. If you specify 0 spare sectors and some sectors fail, you must reformat the flash memory or flash PC card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the flash file system. The Cisco IOS system software contains a monlib file. Use the `show disk0: all` command to display monlib file details.

When this command is used with HSA and you do not specify the `monlib-filename` argument, the system takes the ROM monitor library file from the slave image bundle. If you specify the `monlib-filename` argument, the system assumes that the files reside on the slave devices.

In the command syntax, the `filesystem1:` argument specifies the device to format and the `filesystem2:` argument specifies the optional device containing the monlib file used to format the `filesystem1:` argument. The device determines which monlib file to use, as follows:

- If you omit the optional `filesystem2:` and `monlib-filename` arguments, the system formats the `filesystem1:` argument using the monlib file already bundled with the system software.
- If you omit only the optional `filesystem2:` argument, the system formats the `filesystem1:` argument using the monlib file from the device you specified with the `cd` command.
- If you omit only the optional `monlib-filename` argument, the system formats `filesystem1:` using the `filesystem2:` monlib file.
- When you specify both arguments—`filesystem2:` and `monlib-filename`—the system formats the `filesystem1:` argument using the monlib file from the specified device.
- You can specify the `filesystem1:` argument’s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

**Note**

Most platforms do not support booting from images stored on flash memory cards. You should reboot your device only from integrated memory locations, such as NVRAM.

**Cisco 7600 Series Router Notes**

The `bootflash:`, `slot0:`, `sup-slot0:`, and `sup-bootflash:` keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.
Use the `format` command to format Class A or C flash memory file systems.

- The `disk0:` and `disk1:` keywords are for Class C filesystems.
- The `bootflash:`, `slot0:`, `sup-slot0:`, and `sup-bootflash:` keywords are for Class A filesystems.

The `disk0:` keyword is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

**Cisco ASR 1000 Series Routers Notes**

This command is available in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers.

**Examples**

The following example shows how to format a flash memory card that is inserted in slot 0:

```
Router# format slot0:
Running config file on this device, proceed? [confirm] y
All sectors will be erased, proceed? [confirm] y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the privileged EXEC prompt, the new flash memory card is formatted and ready for use.

This following example shows how to format a CompactFlash PC card that is inserted in slot 0:

```
Router# format disk0:
Running config file on this device, proceed? [confirm] y
All sectors will be erased, proceed? [confirm] y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device disk0 completed
```

When the console returns to the EXEC prompt, the new CompactFlash PC card is formatted and ready for use.

This following example shows how a format operation cleans up the disk and writes the monitor library on the disk filesystem:

```
Router# format formatdisk:
Format operation may take a while. Continue? [confirm] 
Format operation will destroy all data in "bootdisk:". Continue? [confirm]
Hash Computation: 100%Done!
Computed Hash SHA2: DFBA87256310DC8A77BF8158451F7F4
0AC333C9B396D9D0E42DDBD542C30E08
F3946DDE692AF04FDB20F29BE51C49C4
1B631790A542D81F9A7C90ABC2426960

Embedded Hash SHA2: DFBA87256310DC8A77BF8158451F7F4
0AC333C9B396D9D0E42DDBD542C30E08
F3946DDE692AF04FDB20F29BE51C49C4
1B631790A542D81F9A7C90ABC2426960

Digital signature successfully verified in file Monlib
Writing Monlib sectors....
Monlib write complete
Format: All system sectors written. OK...
Format: Total sectors in formatted partition: 1000881
Format: Total bytes in formatted partition: 512451072
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file on a flash memory device.</td>
</tr>
<tr>
<td>show disk0: all</td>
<td>Displays ATA MONLIB file information for disk0.</td>
</tr>
<tr>
<td>show file systems</td>
<td>Lists available file systems.</td>
</tr>
<tr>
<td>squeeze</td>
<td>Permanently deletes flash files by squeezing a Class A flash file system.</td>
</tr>
<tr>
<td>undelete</td>
<td>Recovers a file marked “deleted” on a Class A or Class B flash file system.</td>
</tr>
</tbody>
</table>

**fsck**

To check a File Allocation Table (FAT)-based disk, a flash file system, or a Class C file system for damage and to repair any problems, use the `fsck` command in privileged EXEC or diagnostic mode.

**Supported Platforms Other than the Cisco 7600 Series and Cisco ASR1000 Series Routers**

`fsck [/nocrc] [/automatic] [/all] [/force] [filesystem:]`

**Cisco 7600 Series Routers**

`fsck [/automatic] [/all] [/force] [filesystem:]`

**Cisco ASR 1000 Series Routers**

`fsck [/all] [/force] [filesystem:]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/nocrc</td>
<td>(Optional) This keyword is available for Class C flash file systems only. Omits cyclic redundancy checks (CRCs).</td>
</tr>
<tr>
<td>/automatic</td>
<td>(Optional) This keyword is available for Advanced Technology Attachment (ATA) FAT-based disks only. Specifies that the check and repair actions should proceed automatically. This option can be used to skip the prompts for each check and repair action. This command also specifies the automatic mode for the Cisco 7600 series router; see the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td>/ all</td>
<td>(Optional) Specifies that all partitions on the disk be checked for problems.</td>
</tr>
<tr>
<td>/force</td>
<td>(Optional) Ensures forced termination of simultaneous file operations on the same device.</td>
</tr>
<tr>
<td>filesystem</td>
<td>The file system prefix indicating the disk to be checked. The colon (:) is required. Typically, the file system prefix will be disk0: or disk1:. In case of dual processors, the file system on the redundant supervisor engine can also be specified.</td>
</tr>
</tbody>
</table>
A FAT-based disk, flash file system, or Class C file system is not checked for damage and repaired. If you do not enter the /automatic keyword, command-line interface (CLI) prompts for actions are issued. For the Cisco 7600 series router, if you do not specify the disk0: keyword, the current file system is checked.

This command is available in both privileged EXEC and diagnostic mode on the Cisco ASR1000 series routers.

**Command Modes**

Privileged EXEC (#) Diagnostic (diag)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was implemented on the Cisco 7000 family of routers and on the Cisco 10000 series router and the Gigabit Switch Router (GSR) to support ATA disks.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was modified. Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SX</td>
<td>This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced:</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The /force keyword was added.</td>
</tr>
</tbody>
</table>

**Supported Platforms Other than Cisco 7600 Series Router**

This command performs all steps necessary to remove corrupted files and reclaim unused disk space. Changes include checking for incorrect file sizes, cluster loops, and so on. The default form of this command issues multiple prompts to confirm each of the changes. However, you can skip these prompts by using the /automatic keyword when issuing the command.

When you use the /automatic keyword you are prompted to confirm that you want the automatic option. Prompts for actions will be skipped, but all actions performed are displayed to the terminal (see the example below).

This command works with ATA Personal Computer Memory Card Industry Association (PCMCIA) cards formatted in Disk Operating System (DOS), or for Class C flash file systems.
Only one partition (the active partition) is checked in the ATA disk.

**Cisco 7600 Series Router**

The disk0: or slavedisk0: file systems are the only file systems in the Cisco 7600 series routers on which you can run the File-System-Check (fsck) utility. The slavedisk0: file system appears in redundant supervisor engine systems only.

This command is valid only on Class C flash file systems and only on PCMCIA ATA flash disks and CompactFlash disks.

The output for the **fsck slavedisk0:** command is similar to the **fsck disk0:** command output.

If you do not enter any arguments, the current file system is used. Use the **pwd** command to display the current file system.

If you enter the **disk0:** or **slavedisk0:** keyword, the fsck utility checks the selected file system for problems. If a problem is detected, a prompt is displayed asking if you want the problem fixed.

If you enter the **/automatic** keyword, you are prompted to confirm that you want the automatic mode. In automatic mode, problems are fixed automatically and you are not prompted to confirm.

If you do not specify the **/force** keyword, any simultaneous file operations on the same device are not terminated. Instead, an error message stating files are open for read or write access appears. If you specify the **/force** keyword, the fsck utility terminates files that are open for read or write access and continues to check for problems.

The table below lists the checks and actions that are performed by the fsck utility.

**Table 26: fsck Utility Checks and Actions**

<table>
<thead>
<tr>
<th>Checks</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks the boot sector and the partition table and reports the errors.</td>
<td>No action.</td>
</tr>
<tr>
<td>Validates the media with the signature in the last 2 bytes of the first sector (0x55 and 0xaa, respectively).</td>
<td>No action.</td>
</tr>
<tr>
<td>Checks the os_id to find whether this is a FAT-12 or FAT-16 file system (valid values include 0, 1, 4, and 6).</td>
<td>No action.</td>
</tr>
<tr>
<td>Checks the number of FAT’s field (correct values are 1 and 2).</td>
<td>No action.</td>
</tr>
<tr>
<td>Checks these values:</td>
<td>No action.</td>
</tr>
<tr>
<td>• n_fat_sectors cannot be less than 1.</td>
<td></td>
</tr>
<tr>
<td>• n_root_entries cannot be less than 16.</td>
<td></td>
</tr>
<tr>
<td>• n_root_sectors cannot be less than 2.</td>
<td></td>
</tr>
<tr>
<td>• base_fat_sector, n_sectors_per_cluster, n_heads,</td>
<td></td>
</tr>
<tr>
<td>n_sectors_per_track is not 0.</td>
<td></td>
</tr>
</tbody>
</table>
**Checks**

<table>
<thead>
<tr>
<th>Checks</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks the files and FAT for these errors:</td>
<td>If the cluster is a part of a file chain, the cluster is changed to end of file (EOF). If the cluster is not part of a file chain, it is added to the free list and unused cluster chain. The table below lists valid cluster numbers; numbers other than those listed in the table below are invalid numbers.</td>
</tr>
<tr>
<td>Checks the FAT for invalid cluster numbers.</td>
<td>If the loop is broken, the file is truncated at the cluster where the looping occurred.</td>
</tr>
<tr>
<td>Checks the file’s cluster chain for loops.</td>
<td>If directories are found with nonzero size fields, the size is reset to zero.</td>
</tr>
<tr>
<td>Checks the directories for nonzero size fields.</td>
<td>If the start cluster number of a file is invalid, the file is deleted.</td>
</tr>
<tr>
<td>Checks for invalid start cluster file numbers.</td>
<td>If the file contains bad or free clusters, the file is truncated at the last good cluster; an example is the cluster that points to this bad/free cluster.</td>
</tr>
<tr>
<td>Checks files for bad or free clusters.</td>
<td>If the file’s cluster chain is longer than indicated by the size fields, the file size is recalculated and the directory entry is updated.</td>
</tr>
<tr>
<td>Checks to see if the file’s cluster chain is longer than indicated by the size fields.</td>
<td>If two or more files are crosslinked, you are prompted to accept the repair, and one of the files is truncated.</td>
</tr>
<tr>
<td>Checks to see if two or more files share the same cluster (crosslinked).</td>
<td>If the file’s cluster chain is shorter than is indicated by the size fields, the file size is recalculated and the directory entry is updated.</td>
</tr>
<tr>
<td>Checks to see if the file’s cluster chain is shorter than is indicated by the size fields.</td>
<td>If unused cluster chains are found, new files are created and linked to that file with the name fsck-start cluster</td>
</tr>
<tr>
<td>Checks to see if there are any unused cluster chains.</td>
<td></td>
</tr>
</tbody>
</table>

The table below lists the valid cluster numbers. Numbers other than those listed in the table below are invalid numbers.

**Table 27: Valid Cluster Numbers**

<table>
<thead>
<tr>
<th>Cluster</th>
<th>FAT-12</th>
<th>FAT-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next entry in chain</td>
<td>2-FEF</td>
<td>2-FFEF</td>
</tr>
<tr>
<td>Last entry in chain</td>
<td>FF8-FFF</td>
<td>FFF8-FFFF</td>
</tr>
<tr>
<td>Available cluster</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Cluster</td>
<td>FF7</td>
<td>FFF7</td>
</tr>
</tbody>
</table>

**Examples**

**Supported Platforms Other than the Cisco 7600 Series Router**

The following example shows sample output from the `fsck` command in automatic mode:
Router# fsck /automatic disk1:
Proceed with the automatic mode? [yes] y
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
Start cluster of file disk1:/file1 is invalid, removing file
File disk1:/file2 has a free/bad cluster, truncating...
File disk1:/file2 truncated.
File disk1:/file3 has a free/bad cluster, truncating...
File disk1:/file3 truncated.
File disk1:/file4 has an invalid cluster, truncating...
File disk1:/file4 truncated.
File disk1:/file5 has an invalid cluster, truncating...
File disk1:/file5 truncated.
File disk1:/file6 has an invalid cluster, truncating...
File disk1:/file6 truncated.
File size of disk1:/file7 is not correct, correcting it
File disk1:/file8 cluster chain has a loop, truncating it
File disk1:/file8 truncated.
File disk1:/file9 cluster chain has a loop, truncating it
File disk1:/file9 truncated.
File disk1:/file10 has a free/bad cluster, truncating...
File disk1:/file10 truncated.
File disk1:/file11 has a free/bad cluster, truncating...
File disk1:/file11 truncated.
File disk1:/file12 has a free/bad cluster, truncating...
File disk1:/file12 truncated.
File disk1:/file13 has a free/bad cluster, truncating...
File disk1:/file13 truncated.
File disk1:/file14 has a free/bad cluster, truncating...
File disk1:/file14 truncated.
File disk1:/file15 has a free/bad cluster, truncating...
File disk1:/file15 truncated.
File disk1:/file16 has a free/bad cluster, truncating...
File disk1:/file16 truncated.
Reclaiming unused space...
Created file disk1:/fsck-4 for an unused cluster chain
Created file disk1:/fsck-41 for an unused cluster chain
Created file disk1:/fsck-73 for an unused cluster chain
Created file disk1:/fsck-106 for an unused cluster chain
Created file disk1:/fsck-121 for an unused cluster chain
Created file disk1:/fsck-132 for an unused cluster chain
Created file disk1:/fsck-140 for an unused cluster chain
Created file disk1:/fsck-156 for an unused cluster chain
Created file disk1:/fsck-171 for an unused cluster chain
Created file disk1:/fsck-186 for an unused cluster chain
Created file disk1:/fsck-196 for an unused cluster chain
Created file disk1:/fsck-235 for an unused cluster chain
Created file disk1:/fsck-239 for an unused cluster chain
Updating FAT...
fsck of disk1: complete

Cisco 7600 Series Router

This example shows how to run a check of the current file system:

Router# fsck
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
Files
1) disk0:/FILE3 and
2) disk0:/FILE2
have a common cluster.
Press 1/2 to truncate or any other character to ignore[confirm] q
Ignoring this error and continuing with the rest of the check...
Files
1) disk0:/FILE5 and
2) disk0:/FILE4
have a common cluster.
Press 1/2 to truncate or any other character to ignore[confirm] 1
File disk0:/FILE5 truncated.
Files
1) disk0:/FILE7 and
2) disk0:/FILE6
have a common cluster.

1) disk0:/FILE15 and
2) disk0:/FILE13
have a common cluster.

Press 1/2 to truncate or any other character to ignore[confirm] i

Ignoring this error and continuing with the rest of the check...

Reclaiming unused space...
Created file disk0:/fsck-11 for an unused cluster chain
Created file disk0:/fsck-20 for an unused cluster chain
Created file disk0:/fsck-30 for an unused cluster chain
Created file disk0:/fsck-35 for an unused cluster chain
Created file disk0:/fsck-40 for an unused cluster chain
Created file disk0:/fsck-46 for an unused cluster chain
Created file disk0:/fsck-55 for an unused cluster chain
Created file disk0:/fsck-62 for an unused cluster chain
Created file disk0:/fsck-90 for an unused cluster chain
Updating FAT...
fsck of disk0: complete

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td></td>
<td>pwd</td>
<td>Shows the current setting of the cd command.</td>
</tr>
</tbody>
</table>

**full-help**

To get help for the full set of user-level commands, use the `full-help` command in line configuration mode.

**full-help**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `full-help` command enables (or disables) an unprivileged user to see all of the help messages available. It is used with the `show ?` command.
Examples

In the following example, the `show ?` command is used first with full-help disabled. Then `full-help` is enabled for the line, and the `show ?` command is used again to demonstrate the additional help output that is displayed.

Router> `show ?`
  bootflash Boot Flash information
  calendar Display the hardware calendar
  clock Display the system clock
  context Show context information
dialer Dialer parameters and statistics
history Display the session command history
hosts IP domain-name, lookup style, nameservers, and host table
isdn ISDN information
kerberos Show Kerberos Values
modemcap Show Modem Capabilities database
ppp PPP parameters and statistics
rmon rmon statistics
sessions Information about Telnet connections
snmp snmp statistics
terminal Display terminal configuration parameters
users Display information about terminal lines
version System hardware and software status
Router> `enable`
Password:<letmein>

Router# `configure terminal`
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# `line console 0`
Router(config-line)# `full-help`
Router(config-line)# `exit`

Router% `SYS-5-CONFIG_I: Configured from console by console`
Router# `disable`
Router> `show ?`
  access-expression List access expression
  access-lists List access lists
  aliases Display alias commands
  apollo Apollo network information
  appletalk AppleTalk information
  arp ARP table
  async Information on terminal lines used as router interfaces
  bootflash Boot Flash information
  bridge Bridge Forwarding/Filtering Database [verbose]
  bsc BSC interface information
  bstun BSTUN interface information
  buffers Buffer pool statistics
  calendar Display the hardware calendar
  .
  .
  translate Protocol translation information
ttycap Terminal capability tables
users Display information about terminal lines
version System hardware and software status
vines VINES information
vlans Virtual LANs Information
whoami Info on current tty line
x25 X.25 information
xns XNS information
xremote XRemote statistics
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Displays a brief description of the help system.</td>
</tr>
</tbody>
</table>

**help**

To display a brief description of the help system, use the `help` command in any command mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

- User EXEC
- Privileged EXEC
- All configuration modes

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `help` command provides a brief description of the context-sensitive help system, which functions as follows:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called `word help`, because it lists only the keywords or arguments that begin with the abbreviation you entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called `command syntax help`, because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.

**Examples**

In the following example, the `help` command is used to display a brief description of the help system:

```
Router# help
Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options. Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
```
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr').

The following example shows how to use word help to display all the privileged EXEC commands that begin with the letters “co.” The letters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command.

```
Router# co?
configure connect copy
Router# co
```

The following example shows how to use command syntax help to display the next argument of a partially complete **access-list** command. One option is to add a wildcard mask. The <cr> symbol indicates that the other option is to press Enter to execute the command without adding any more keywords or arguments. The characters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command or to execute the command as it is.

```
Router(config)# access-list 99 deny 131.108.134.234 ?
A.B.C.D Mask of bits to ignore <cr>
Router(config)# access-list 99 deny 131.108.134.234
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full-help</td>
<td>Enables help for the full set of user-level commands for a line.</td>
</tr>
</tbody>
</table>

### hidekeys

To suppress the display of password information in configuration log files, use the **hidekeys** command in configuration change logger configuration mode. To allow the display of password information in configuration log files, use the **no** form of this command.

**hidekeys**

**no hidekeys**

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

Password information is displayed.

#### Command Modes

Configuration change logger configuration (config-archive-log-config)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
**Modification Release**

This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.

This command was integrated into Cisco IOS XE Release 3.9S.

**Usage Guidelines**

Enabling the `hidekeys` command increases security by preventing password information from being displayed in configuration log files.

**Examples**

The following example shows how to prevent password information from being displayed in configuration log files:

```
Device# configure terminal
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# hidekeys
Device(config-archive-log-config)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>archive</code></td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td><code>log config</code></td>
<td>Enters configuration change logger configuration mode.</td>
</tr>
<tr>
<td><code>logging enable</code></td>
<td>Enables the logging of configuration changes.</td>
</tr>
<tr>
<td><code>logging size</code></td>
<td>Specifies the maximum number of entries retained in the configuration log.</td>
</tr>
<tr>
<td><code>notify syslog</code></td>
<td>Enables the sending of notifications of configuration changes to a remote syslog.</td>
</tr>
<tr>
<td><code>show archive log config</code></td>
<td>Displays entries from the configuration log.</td>
</tr>
</tbody>
</table>

**history**

To enable the command history function, use the `history` command in line configuration mode. To disable the command history function, use the `no` form of this command.

```
history
no history
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Enabled with ten command lines in the buffer.

**Command Modes**

Line configuration
The command history function provides a record of EXEC commands that you have entered. This function is particularly useful for recalling long or complex commands or entries, including access lists.

To change the number of command lines that the system will record in its history buffer, use the `history size` line configuration command.

The `history` command enables the history function with the last buffer size specified or, if there was not a prior setting, with the default of ten lines. The `no history` command disables the history function.

The `show history` EXEC command will list the commands you have entered, but you can also use your keyboard to display individual commands. The table below lists the keys you can use to recall commands from the command history buffer.

### Table 28: History Keys

<table>
<thead>
<tr>
<th>Key(s)</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or Up Arrow(^2)</td>
<td>Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or Down Arrow(^1)</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
</tbody>
</table>

\(^2\) The arrow keys function only with ANSI-compatible terminals.

### Examples

In the following example, the command history function is disabled on line 4:

```
Router(config)# line 4
Router(config-line)# no history
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>history size</code></td>
<td>Sets the command history buffer size for a particular line.</td>
</tr>
<tr>
<td><code>show history</code></td>
<td>Lists the commands you have entered in the current EXEC session.</td>
</tr>
<tr>
<td><code>terminal history</code></td>
<td>Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.</td>
</tr>
</tbody>
</table>
**History Size**

To change the command history buffer size for a particular line, use the `history size` command in line configuration mode. To reset the command history buffer size to ten lines, use the `no history size` command.

```
history size number-of-lines
no history size
```

**Syntax Description**

| number-of-lines | Specifies the number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10. |

**Command Default**

10 command lines

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `history size` command should be used in conjunction with the `history` and `show history` commands. The `history` command enables or disables the command history function. The `show history` command lists the commands you have entered in the current EXEC session. The number of commands that the history buffer will show is set by the `history size` command.

**Note**

The `history size` command only sets the size of the buffer; it does not reenable the history function. If the `no history` command is used, the `history` command must be used to reenable this function.

**Examples**

The following example displays line 4 configured with a history buffer size of 35 lines:

```
Router(config)# line 4
Router(config-line)# history size 35
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>history</code></td>
<td>Enables or disables the command history function.</td>
</tr>
<tr>
<td><code>show history</code></td>
<td>Lists the commands you have entered in the current EXEC session.</td>
</tr>
<tr>
<td><code>terminal history size</code></td>
<td>Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.</td>
</tr>
</tbody>
</table>
hold-character

To define the local hold character used to pause output to the terminal screen, use the hold-character command in line configuration mode. To restore the default, use the no form of this command.

```
hold-character ascii-number
no hold-character
```

**Syntax Description**
- `ascii-number` ASCII decimal representation of a character or control sequence (for example, Ctrl-P).

**Command Default**
No hold character is defined.

**Command Modes**
Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The Break character is represented by zero; NULL cannot be represented. To continue the output, enter any character after the hold character. To use the hold character in normal communications, precede it with the escape character. See the “ASCII Character Set” appendix for a list of ASCII characters.

**Examples**
The following example sets the hold character to Ctrl-S, which is ASCII decimal character 19:

```
Router(config)# line 8
Router(config-line)# hold-character 19
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal hold-character</td>
<td>Sets or changes the hold character for the current session.</td>
</tr>
</tbody>
</table>

hostname

To specify or modify the hostname for the network server, use the hostname command in global configuration mode.

```
hostname name
```

**Syntax Description**
- `name` New hostname for the network server.

**Command Default**
The default hostname is Router.

**Command Modes**
Global configuration
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was integrated into Cisco IOS XE Release 2.5.</td>
</tr>
<tr>
<td>15.0(1)M4</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M4 and support for numeric hostnames added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The hostname is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer*.

The name must also follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.

```bash
Router(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

A hostname of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names--Implementation and Specification*.

On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the hostname of “Router,” you will only see the following prompt (on most systems):

```
Router(config-service-profile)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the `hostname` global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign hostnames of no more than nine characters.
The use of a special character such as \\ (backslash) and a three or more digit number for the character setting like hostname, results in incorrect translation:

```
Router(config)#
Router(config)#hostname \99
% Hostname contains one or more illegal characters.
```

### Examples

The following example changes the hostname to “host1”:

```
Router(config)# hostname host1
host1(config)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setup</td>
<td>Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.</td>
</tr>
</tbody>
</table>

### hw-module reset

To reset a module by turning the power off and then on, use the `hw-module reset` command in privileged EXEC mode.

```
hw-module module num reset
```

#### Syntax Description

- **module num**: Applies the command to a specific module; see the “Usage Guidelines” section for valid values.

#### Command Default

This command has no default settings.

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The `num` argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

#### Examples

This example shows how to reload a specific module:

```
Router#
hw-module module 3 reset
```
hw-module shutdown

To shut down the module, use the **hw-module shutdown** command in privileged EXEC mode.

**hw-module module num shutdown**

**Syntax Description**

| module num | Applies the command to a specific module; see the “Usage Guidelines” section for valid values. |

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SX</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported on the SSL Services Module and the NAM.

If you enter the hw-module **shutdown** command to shut down the module, you will have to enter the no power enable module command and the **power enable module** command to restart (power down and then power up) the module.

**Examples**

This example shows how to shut down and restart the module:

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

insecure

To configure a line as insecure, use the **insecure** command in line configuration mode. To disable this function, use the **no** form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to identify a modem line as insecure for DEC local area transport (LAT) classification.

Examples

In the following example, line 10 is configured as an insecure dialup line:

Router(config)# line 10
Router(config-line)# insecure

install

To install Software Maintenance Upgrade (SMU) packages, use the install command in privileged EXEC mode.


Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abort</td>
<td>Aborts the current install operation.</td>
</tr>
<tr>
<td>activate</td>
<td>Validates whether the SMU is added through the install add command.</td>
</tr>
<tr>
<td></td>
<td>This keyword runs a compatibility check, updates package status, and if the</td>
</tr>
<tr>
<td></td>
<td>package can be restarted, it triggers post-install scripts to restart the</td>
</tr>
<tr>
<td></td>
<td>necessary processes, or triggers a reload for non-restartable packages.</td>
</tr>
<tr>
<td>file</td>
<td>Specifies the package to be activated.</td>
</tr>
<tr>
<td>{bootflash:</td>
<td>flash:</td>
</tr>
<tr>
<td>auto-abort-timer</td>
<td>(Optional) Installs an auto-abort timer.</td>
</tr>
<tr>
<td>timer</td>
<td>The timer is set by the activate keyword and removed by the commit keyword.</td>
</tr>
<tr>
<td></td>
<td>After the expiry of the install auto-abort timer command, a device can be</td>
</tr>
<tr>
<td></td>
<td>rolled back to a stage before the install commit command is used.</td>
</tr>
</tbody>
</table>
**prompt-level {all | none}**

(Optional) Prompts the user about installation activities.

For example, the **activate** keyword, automatically triggers a reload for packages that require a reload. Before activating the package, a message will prompt users as to whether they want to continue.

The **all** keyword allows you to enable prompts. The **none** keyword disable prompts.

**add**

Copies files from a remote location (via FTP, TFTP) to a device and performs Software Maintenance Upgrade (SMU) compatibility check for the platform and image versions.

This keyword runs base compatibility checks to ensure that a specified package is supported on a platform. It also adds an entry in the package file, so that the status can be monitored and maintained.


**commit**

Makes SMU changes persistent over reloads.

You can do a commit after activating a package, while the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.

**auto-abort-timer stop**

Stops the auto-abort timer.

If the rollback timer is not stopped through the command, the device rolls back to an older software version when rollback timer expires. Default: 120 minutes.

**deactivate**

Deactivates an installed package.

Deactivating a package also updates the package status and triggers a process restart or a reload.

**label id**

Specifies the id of the install point to label.

**description**

Adds a description to specified install point.

**label-name name**

Adds a description to specified install point.

**remove**

Remove installed packages.

The package file is removed from the file system. The **remove** keyword can only be used on packages that are currently inactive.

**inactive**

Removes all inactive packages from the device.
rollback
Rollbacks the SMU package to the base version, the last committed version, or a known commit ID.

to base
Returns to the base image.

committed
Returns to the installation state when the last commit operation was performed.

id install-ID
Returns to the specific install point ID.
Valid values are from 1 to 4294967295.

Command Default
Packages are not installed.

Command Modes
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
An SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. This package contain a minimal set of files for patching the release along with some metadata that describes the contents of the package.

Packages must be added prior to activating the SMU.

A package must be deactivated, before it is removed from the device.

Example
The following example shows how to add an install package on a device:

```
Device# install add file tftp://172.16.0.1//tftpboot/folder1/isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
```

```
install_add: START Sun Feb 26 05:57:04 UTC 2017
Downloading file tftp://172.16.0.1//tftpboot/folder1/isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
SUCCESS: install_add /bootflash/isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
```

The following example shows how to activate an install package:

```
Device# install activate file bootflash:isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
```

```
install_activate: START Sun Feb 26 05:58:41 UTC 2017
DMP package.
Netconf processes stopped
SUCCESS: install_activate /bootflash/isr4300-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
Sun Feb 26 05:58:58 UTC 2017
```
The following example shows how to commit an installed package:

Device# **install commit**

install_commit: START Sun Feb 26 06:46:48 UTC 2017
SUCCESS: install_commit Sun Feb 26 06:46:52 UTC 2017

The following example shows how to rollback to the base SMU package:

Device# **install rollback to base**

install_rollback: START Sun Feb 26 06:50:29 UTC 2017
7 install_rollback: Restarting impacted processes to take effect
7 install_rollback: restarting confd

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show install</td>
<td>Displays information about install packages.</td>
</tr>
</tbody>
</table>

**international**

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^), use the **international** command in line configuration mode. To display characters in 7-bit format, use the **no** form of this command.

**international**
**no international**
syntax description

this command has no arguments or keywords.

command default

disabled

command modes

line configuration

command history

<table>
<thead>
<tr>
<th>release</th>
<th>modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>this command was introduced.</td>
</tr>
<tr>
<td>12.2(33)sra</td>
<td>this command was integrated into cisco ios release 12.2(33)sra.</td>
</tr>
</tbody>
</table>

usage guidelines

if you are configuring a cisco ios platform using the cisco web browser user interface (ui), this function is enabled automatically when you enable the cisco web browser ui using the ip http server global configuration command.

examples

the following example enables a cisco ios platform to display 8-bit and multibyte characters and print the escape character as a single character instead of as the caret and bracket symbols (^[) when you are using telnet to access the platform:

    line vty 4
    international

related commands

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal international</td>
<td>prints the escape character as a single character instead of as the caret and bracket symbols (^[) for a current telnet session in instances when you are using telnet to access a cisco ios platform and you want to display 8-bit and multibyte international characters (for example, kanji).</td>
</tr>
</tbody>
</table>

ip bootp server

ip bootp server

no ip bootp server

syntax description

this command has no arguments or keywords.

command default

enabled

command modes

global configuration

command history

<table>
<thead>
<tr>
<th>release</th>
<th>modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>this command was introduced.</td>
</tr>
</tbody>
</table>
Release | Modification
--- | ---
12.0(1)T | The DHCP relay agent and DHCP server features were introduced. BOOTP forwarding is now handled by the DHCP relay agent implementation.
12.2(8)T | The `ip dhcp bootp ignore` command was introduced.
12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines**

By default, the BOOTP service is enabled. When disabled, the `no ip bootp server` command will appear in the configuration file.

The integrated Dynamic Host Configuration Protocol (DHCP) server was introduced in Cisco IOS Release 12.0(1)T. Because DHCP is based on BOOTP, both of these services share the “well-known” UDP server port of 67 (per RFC 951, RFC 1534, and RFC 2131; the client port is 68). To disable DHCP services (DHCP relay and DHCP server), use the `no service dhcp` command. To disable BOOTP services (in releases 12.2(8)T and later), but leave DHCP services enabled, use the `ip dhcp bootp ignore` command.

If both the BOOTP server and DHCP server are disabled, “ICMP port unreachable” messages will be sent in response to incoming requests on port 67, and the original incoming packet will be discarded. If DHCP is enabled, using the `no ip bootp server` command by itself will not stop the router from listening on UDP port 67.

**Note**

As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network. Any network device that has User Data Protocol (UDP), TCP, BOOTP, DHCP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

**Examples**

In the following example, BOOTP and DHCP services are disabled on the router:

```
Router(config)# no ip bootp server
Router(config)# no service dhcp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dhcp bootp ignore</code></td>
<td>Configures the Cisco IOS DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets, allowing you continue using DHCP while disabling BOOTP.</td>
</tr>
<tr>
<td><code>service dhcp</code></td>
<td>Enables the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent features.</td>
</tr>
</tbody>
</table>

**`ip finger`**

To configure a system to accept Finger protocol requests (defined in RFC 742), use the `ip finger` command in global configuration mode. To disable this service, use the `no` form of this command.
**ip finger [rfc-compliant]**

**no ip finger**

**Syntax Description**

| rfc-compliant | (Optional) Configures the system to wait for “Return” or “/W” input when processing Finger requests. This keyword should not be used for those systems. |

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5), 12.1(5)T</td>
<td>This command was changed from being enabled by default to being disabled by default.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Finger service allows remote users to view the output equivalent to the `show users [wide]` command.

When `ip finger` is configured, the router will respond to a `telnet a.b.c.d finger` command from a remote host by immediately displaying the output of the `show users` command and then closing the connection.

When the `ip finger rfc-compliant` command is configured, the router will wait for input before displaying anything (as required by RFC 1288). The remote user can then enter the Return key to display the output of the `show users` EXEC command, or enter /W to display the output of the `show users wide` EXEC command. After this information is displayed, the connection is closed.

**Note**

As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Because of the potential for hung lines, the `rfc-compliant` form of this command should not be configured for devices with more than 20 simultaneous users.

**Examples**

The following example disables the Finger protocol:

```
Router(config)# no ip finger
```

**ip ftp passive**

To configure the router to use only passive FTP connections, use the `ip ftp passive` command in global configuration mode. To allow all types of FTP connections, use the `no` form of this command.

```
ip ftp passive
no ip ftp passive
```
Syntax Description
This command has no arguments or keywords.

Command Default
All types of FTP connections are allowed.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples
In the following example, the router is configured to use only passive FTP connections:

Router(config)# ip ftp passive

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ftp password</td>
<td>Specifies the password to be used for FTP connections.</td>
</tr>
<tr>
<td>ip ftp source-interface</td>
<td>Specifies the source IP address for FTP connections.</td>
</tr>
<tr>
<td>ip ftp username</td>
<td>Configures the username for FTP connections.</td>
</tr>
</tbody>
</table>

ip ftp password

To specify the password to be used for File Transfer Protocol (FTP) connections, use the ip ftp password command in global configuration mode. To return the password to its default, use the no form of this command.

ip ftp password [type] password
no ip ftp password

Syntax Description

<table>
<thead>
<tr>
<th>type</th>
<th>(Optional) Type of encryption to use on the password. A value of 0 disables encryption. A value of 7 indicates proprietary encryption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>Password to use for FTP connections.</td>
</tr>
</tbody>
</table>

Command Default
The router forms a password username@routername.domain. The variable username is the username associated with the current session, routername is the configured host name, and domain is the domain of the router.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Cisco IOS Configuration Fundamentals Command Reference
Any software that supports RFC1738 does not allow username, path, or filename with pattern %xy, where (where x and y are any two hexa values 0-f, 0-F)

Examples

The following example configures the router to use the username “red” and the password “blue” for FTP connections:

Router(config)# ip ftp username red
Router(config)# ip ftp password blue

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ftp password</td>
<td>Specifies the password to be used for FTP connections.</td>
</tr>
<tr>
<td>ip ftp source-interface</td>
<td>Specifies the source IP address for FTP connections.</td>
</tr>
<tr>
<td>ip ftp username</td>
<td>Configures the username for FTP connections.</td>
</tr>
</tbody>
</table>

ip ftp source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ip ftp source-interface** command in global configuration mode. To use the address of the interface where the connection is made, use the **no** form of this command.

**ip ftp source-interface** interface-type interface-number
**no ip ftp source-interface**

**Syntax Description**

| interface-type interface-number | The interface type and number to use to obtain the source address for FTP connections. |

**Command Default**

The FTP source address is the IP address of the interface that the FTP packets use to leave the router.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(6)</td>
<td>Destination address lookup in a Virtual Private Network (VPN) routing and forwarding (VRF) table was added for the transfer of FTP packets.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(8)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use this command to set the same source address for all FTP connections.

In Cisco IOS 12.3(6) and later releases, FTP is VRF-aware, which means that FTP transfer is supported across an interface within a VRF instance. To specify a VRF as a source for FTP connections, the VRF must be associated with the same interface that you configure with the `ip ftp source-interface` command. In this configuration, FTP looks for the destination IP address for file transfer in the specified VRF table. If the specified source interface is not up, Cisco IOS software selects the address of the interface closest to the destination as the source address.

Examples

The following example shows how to configure the router to use the IP address associated with Ethernet interface 0 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
Router> enable
Router# configure terminal
Router(config)# ip ftp source-interface ethernet 0
```

The following example shows how to configure the router to use the VRF table named vpn1 to look for the destination IP address for the transfer of FTP packets:

```
Router# configure terminal
Router(config)# ip ftp source-interface ethernet 0
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target both 200:1
Router(config-vrf)# interface ethernet 0
Router(config-if)# ip vrf forwarding vpn1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ftp passive</code></td>
<td>Configures the router to use only passive FTP connections.</td>
</tr>
<tr>
<td><code>ip ftp password</code></td>
<td>Specifies the password to be used for FTP connections.</td>
</tr>
<tr>
<td><code>ip ftp username</code></td>
<td>Configures the username for FTP connections.</td>
</tr>
</tbody>
</table>

**ip ftp username**

To configure the username for File Transfer Protocol (FTP) connections, use the `ip ftp username` command in global configuration mode. To configure the router to attempt anonymous FTP, use the `no` form of this command.

```
ip ftp username username
no ip ftp username
```

**Syntax Description**

- `username`: Username for FTP connections.

**Command Default**

The Cisco IOS software attempts an anonymous FTP.

**Command Modes**

Global configuration
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The remote username must be associated with an account on the destination server.

**Examples**

In the following example, the router is configured to use the username “red” and the password “blue” for FTP connections:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ftp passive</td>
<td>Configures the router to use only passive FTP connections.</td>
</tr>
<tr>
<td>ip ftp password</td>
<td>Specifies the password to be used for FTP connections.</td>
</tr>
<tr>
<td>ip ftp source-interface</td>
<td>Specifies the source IP address for FTP connections.</td>
</tr>
</tbody>
</table>

**ip rarp-server**

To enable the router to act as a Reverse Address Resolution Protocol (RARP) server, use the `ip rarp-server` command in interface configuration mode. To restore the interface to the default of no RARP server support, use the `no` form of this command.

```
ip rarp-server ip-address
no ip rarp-server ip-address
```

**Syntax Description**

| ip-address          | IP address that is to be provided in the source protocol address field of the RARP response packet. Normally, this is set to whatever address you configure as the primary address for the interface. |

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This feature makes diskless booting of clients possible between network subnets where the client and server are on separate subnets.

RARP server support is configurable on a per-interface basis, so that the router does not interfere with RARP traffic on subnets that need no RARP assistance.

The Cisco IOS software answers incoming RARP requests only if both of the following two conditions are met:

- The `ip rarp-server` command has been configured for the interface on which the request was received.
- A static entry is found in the IP ARP table that maps the MAC address contained in the RARP request to an IP address.

Use the `show ip arp` EXEC command to display the contents of the IP ARP cache.

Sun Microsystems, Inc. makes use of RARP and UDP-based network services to facilitate network-based booting of SunOS on its workstations. By bridging RARP packets and using both the `ip helper-address` interface configuration command and the `ip forward-protocol` global configuration command, the Cisco IOS software should be able to perform the necessary packet switching to enable booting of Sun workstations across subnets. Unfortunately, some Sun workstations assume that the sender of the RARP response, in this case the router, is the host that the client can contact to TFTP load the bootstrap image. This causes the workstations to fail to boot.

By using the `ip rarp-server` command, the Cisco IOS software can be configured to answer these RARP requests, and the client machine should be able to reach its server by having its TFTP requests forwarded through the router that acts as the RARP server.

In the case of RARP responses to Sun workstations attempting to diskless boot, the IP address specified in the `ip rarp-server` interface configuration command should be the IP address of the TFTP server. In addition to configuring RARP service, the Cisco IOS software must be configured to forward UDP-based Sun portmapper requests to completely support diskless booting of Sun workstations. This can be accomplished using configuration commands of the following form:

```
ip forward-protocol udp 111
interface interface name
ip helper-address target-address
```

RFC 903 documents the RARP.

Examples

The following partial example configures a router to act as a RARP server. The router is configured to use the primary address of the specified interface in its RARP responses.

```
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
ip address 172.30.3.100 255.255.255.0
ip rarp-server 172.30.3.100
```

In the following example, a router is configured to act as a RARP server, with TFTP and portmapper requests forwarded to the Sun server:

```
! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
```
interface ethernet 0
! Configure the router to act as a RARP server, using the Sun Server's IP address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip forward-protocol</td>
<td>Speeds up flooding of UDP datagrams using the spanning-tree algorithm.</td>
</tr>
<tr>
<td>ip helper-address</td>
<td>Forwards UDP broadcasts, including BOOTP, received on an interface.</td>
</tr>
</tbody>
</table>

### ip rcmd domain-lookup

To reenable the basic Domain Name Service (DNS) security check for rcp and rsh, use the **ip rcmd domain-lookup** command in global configuration mode. To disable the basic DNS security check for remote copy protocol (rcp) and remote shell protocol (rsh), use the **no** form of this command.

```plaintext
ip rcmd domain-lookup
no ip rcmd domain-lookup
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

Enabled

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The abbreviation RCMD (remote command) is used to indicate both rsh and rcp.

DNS lookup for RCMD is enabled by default (provided general DNS services are enabled on the system using the **ip domain-lookup** command).

The **no ip rcmd domain-lookup** command is used to disable the DNS lookup for RCMD. The **ip rcmd domain-lookup** command is used to reenable the DNS lookup for RCMD.

DNS lookup for RCMD is performed as a basic security check. This check is performed using a host authentication process. When enabled, the system records the address of the requesting client. That address is mapped to a host name using DNS. Then a DNS request is made for the IP address for that host name. The IP address received is then checked against the original requesting address. If the address does not match with any of the addresses received from DNS, the RCMD request will not be serviced.

This reverse lookup is intended to help protect against spoofing. However, please note that the process only confirms that the IP address is a valid “routable” address; it is still possible for a hacker to spoof the valid IP address of a known host.
The DNS lookup is done after the TCP handshake but before the router (which is acting as a rsh/rcp server) sends any data to the remote client.

The `no ip rcmd domain-lookup` will turn off DNS lookups for rsh and rcp only. The `no ip domain-lookup` command takes precedence over the `ip rcmd domain-lookup` command. This means that if the `no ip domain-lookup` command is in the current configuration, DNS will be bypassed for rcp and rsh even if the `ip rcmd domain-lookup` command is enabled.

**Examples**

In the following example, the DNS security check is disabled for RCMD (rsh/rcp):

```
Router(config)# no ip rcmd domain-lookup
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-lookup</td>
<td>Enables the IP DNS-based host name-to-address translation.</td>
</tr>
</tbody>
</table>

**ip rcmd rcp-enable**

To configure the Cisco IOS software to allow remote users to copy files to and from the router using remote copy protocol (rcp), use the `ip rcmd rcp-enable` command in global configuration mode. To disable rcp on the device, use the `no` form of this command.

```
ip rcmd rcp-enable
no ip rcmd rcp-enable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

To ensure security, the router is not enabled for rcp by default.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To allow a remote user to execute rcp commands on the router, you must also create an entry for the remote user in the local authentication database using the `ip rcmd remote-host` command.

The `no ip rcmd rcp-enable` command does not prohibit a local user from using rcp to copy system images and configuration files to and from the router.

To protect against unauthorized users copying the system image or configuration files, the router is not enabled for rcp by default.

**Examples**

In the following example, the rcp service is enabled on the system, the IP address assigned to the Loopback0 interface is used as the source address for outbound rcp and rsh packets, and access is granted to the user “netadmin3” on the remote host 172.16.101.101:
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rcmd remote-host</td>
<td>Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.</td>
</tr>
</tbody>
</table>

**ip rcmd remote-host**

To create an entry for the remote user in a local authentication database so that remote users can execute commands on the router using remote shell protocol (rsh) or remote copy protocol (rcp), use the `ip rcmd remote-host` command in global configuration mode. To remove an entry for a remote user from the local authentication database, use the `no` form of this command.

```
ip rcmd remote-host local-username {ip-address host-name} remote-username [enable [level]]
no ip rcmd remote-host local-username {ip-address host-name} remote-username [enable [level]]
```

**Syntax Description**

- `local-username` Name of the user on the local router. You can specify the router name as the username. This name needs to be communicated to the network administrator or to the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
- `ip-address` IP address of the remote host from which the local router will accept remotely executed commands. Either the IP address or the host name is required.
- `host-name` Name of the remote host from which the local router will accept remotely executed commands. Either the host name or the IP address is required.
- `remote-username` Name of the user on the remote host from which the router will accept remotely executed commands.
- `enable [level]` (Optional) Enables the remote user to execute privileged EXEC commands using rsh or to copy files to the router using rcp. The range is from 1 to 15. The default is 15. For information on the enable level, refer to the `privilege level` global configuration command in the Release 12.2 Cisco IOS Security Command Reference.

**Command Default**

No entries are in the local authentication database.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
A TCP connection to a router is established using an IP address. Using the host name is valid only when you are initiating an rcp or rsh command from a local router. The host name is converted to an IP address using DNS or host-name aliasing.

To allow a remote user to execute rcp or rsh commands on a local router, you must create an entry for the remote user in the local authentication database. You must also enable the router to act as an rsh or rcp server.

To enable the router to act as an rsh server, issue the `ip rcmd rsh-enable` command. To enable the router to act as an rcp server, issue the `ip rcmd rcp-enable` command. The router cannot act as a server for either of these protocols unless you explicitly enable the capacity.

A local authentication database, which is similar to a UNIX `.rhosts` file, is used to enforce security on the router through access control. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user. To permit a remote user of rsh to execute commands in privileged EXEC mode or to permit a remote user of rcp to copy files to the router, specify the `enable` keyword and level. For information on the enable level, refer to the `privilege level` global configuration command in the Release 12.2 Cisco IOS Security Command Reference.

An entry that you configure in the authentication database differs from an entry in a UNIX `.rhosts` file in the following aspect. Because the `.rhosts` file on a UNIX system resides in the home directory of a local user account, an entry in a UNIX `.rhosts` file need not include the local username; the local username is determined from the user account. To provide equivalent support on a router, specify the local username along with the remote host and remote username in each authentication database entry that you configure.

For a remote user to be able to execute commands on the router in its capacity as a server, the local username, host address or name, and remote username sent with the remote client request must match values configured in an entry in the local authentication file.

A remote client host should be registered with DNS. The Cisco IOS software uses DNS to authenticate the remote host’s name and address. Because DNS can return several valid IP addresses for a host name, the Cisco IOS software checks the address of the requesting client against all of the IP addresses for the named host returned by DNS. If the address sent by the requester is considered invalid, that is, it does not match any address listed with DNS for the host name, then the software will reject the remote-command execution request.

Note that if no DNS servers are configured for the router, then that device cannot authenticate the host in this manner. In this case, the Cisco IOS software sends a broadcast request to attempt to gain access to DNS services on another server. If DNS services are not available, you must use the `no ip domain-lookup` command to disable the attempt to gain access to a DNS server by sending a broadcast request.

If DNS services are not available and, therefore, you bypass the DNS security check, the software will accept the request to remotely execute a command only if all three values sent with the request match exactly the values configured for an entry in the local authentication file.

### Examples

The following example allows the remote user named `netadmin3` on a remote host with the IP address 172.16.101.101 to execute commands on `router1` using the rsh or rcp protocol. User `netadmin3` is allowed to execute commands in privileged EXEC mode.

```
Router(config)# ip rcmd remote-host router1 172.16.101.101 netadmin3 enable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip rcmd rcp-enable</code></td>
<td>Configures the Cisco IOS software to allow remote users to copy files to and from the router.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip domain-lookup</td>
<td>Enables the IP DNS-based host name-to-address translation.</td>
</tr>
<tr>
<td>ip rcmd rsh-enable</td>
<td>Configures the router to allow remote users to execute commands on it using the rsh protocol.</td>
</tr>
</tbody>
</table>

**ip rcmd remote-username**

To configure the remote username to be used when requesting a remote copy using remote copy protocol (rcp), use the `ip rcmd remote-username` command in global configuration mode. To remove from the configuration the remote username, use the `no` form of this command.

```
ip rcmd remote-username username
no ip rcmd remote-username username
```

**Syntax Description**

<table>
<thead>
<tr>
<th>username</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>username</strong></td>
<td>Name of the remote user on the server. This name is used for rcp copy requests. All files and images to be copied are searched for or written relative to the directory of the remote user’s account, if the server has a directory structure, for example, as do UNIX systems.</td>
</tr>
</tbody>
</table>

**Command Default**

If you do not issue this command, the Cisco IOS software sends the remote username associated with the current tty process, if that name is valid, for rcp copy commands. For example, if the user is connected to the router through Telnet and the user was authenticated through the `username` command, then the software sends that username as the remote username.

**Note**

The remote username must be associated with an account on the destination server.

If the username for the current tty process is not valid, the Cisco IOS software sends the host name as the remote username. For rcp boot commands, the Cisco IOS software sends the access server host name by default.

**Note**

For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called tty devices (tty stands for teletype, the original UNIX terminal).

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The rcp protocol requires that a client send the remote username on an rcp request to the server. Use this command to specify the remote username to be sent to the server for an rcp copy request. If the server has a
directory structure, as do UNIX systems, all files and images to be copied are searched for or written relative to the directory of the remote user’s account.

Cisco IOS Release 10.3 added the `ip` keyword to `rcmd` commands. If you are upgrading from Release 10.2 to Release 10.3 or a later release, this keyword is automatically added to any `rcmd` commands you have in your Release 10.2 configuration files.

Examples

The following example configures the remote username to netadmin1:

```
Router(config) ip rcmd remote-username netadmin1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>boot network rcp</code></td>
<td>Changes the default name of the network configuration file from which to load configuration commands.</td>
</tr>
<tr>
<td><code>boot system rcp</code></td>
<td>Specifies the system image that the router loads at startup.</td>
</tr>
<tr>
<td><code>bridge acquire</code></td>
<td>Forwards any frames for stations that the system has learned about dynamically.</td>
</tr>
<tr>
<td><code>copy</code></td>
<td>Copies any file from a source to a destination.</td>
</tr>
</tbody>
</table>

`ip rcmd rsh-enable`

To configure the router to allow remote users to execute commands on it using remote shell protocol (rsh), use the `ip rcmd rsh-enable` command in global configuration mode. To disable a router that is enabled for rsh, use the `no` form of this command.

```
ip rcmd rsh-enable
no ip rcmd rsh-enable
```

Syntax Description

This command has no arguments or keywords.

Command Default

To ensure security, the router is not enabled for rsh by default.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

rsh, used as a client process, gives users the ability to remotely get router information (such as status) without the need to connect into the router and then disconnect. This is valuable when looking at many statistics on many different routers.
Use this command to enable the router to receive rsh requests from remote users. In addition to issuing this command, you must create an entry for the remote user in the local authentication database to allow a remote user to execute rsh commands on the router.

The `no ip rcmd rsh-enable` command does not prohibit a local user of the router from executing a command on other routers and UNIX hosts on the network using rsh. The no form of this command only disables remote access to rsh on the router.

**Examples**

The following example enables a router as an rsh server:

```
Router(config)# ip rcmd rsh-enable
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip rcmd remote-host</td>
<td>Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.</td>
</tr>
</tbody>
</table>

**ip rcmd source-interface**

To force remote copy protocol (rcp) or remote shell protocol (rsh) to use the IP address of a specified interface for all outgoing rcp/rsh communication packets, use the `ip rcmd source-interface` command in global configuration mode. To disable a previously configured `ip rcmd source-interface` command, use the `no` form of this command.

```
ip rcmd source-interface interface-id
no ip rcmd source-interface interface-id
```

**Syntax Description**

- `interface-id`: The name and number used to identify the interface. For example, Loopback2.

**Command Default**

The address of the interface closest to the destination is used as the source interface for rcp/rsh communications.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If this command is not used, or if the interface specified in this command is not available (not up), the Cisco IOS software uses the address of the interface closest to the destination as the source address.

Use this command to force the system to tag all outgoing rcp/rsh packets with the IP address associated with the specified interface. This address is used as the source address as long as the interface is in the up state.

This command is especially useful in cases where the router has many interfaces, and you want to ensure that all rcp and/or rsh packets from this router have the same source IP address. A consistent address is preferred.
so that the other end of the connection (the rcp/rsh server or client) can maintain a single session. The other benefit of a consistent address is that an access list can be configured on the remote device.

The specified interface must have an IP address associated with it. If the specified interface does not have an IP address or is in a down state, then rcp/rsh reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.

### Examples

In the following example, Loopback interface 0 is assigned an IP address of 220.144.159.200, and the `ip rcmd source-interface` command is used to specify that the source IP address for all rcp/rsh packets will be the IP address assigned to the Loopback0 interface:

```
interface Loopback0
  description Loopback interface
  ip address 220.144.159.200 255.255.255.255
  no ip directed-broadcast

  clock timezone GMT 0
  ip subnet-zero
  no ip source-route
  no ip finger
  ip rcmd source-interface Loopback0
  ip telnet source-interface Loopback0
  ip tftp source-interface Loopback0
  ip ftp source-interface Loopback0
  ip ftp username cisco
  ip ftp password shhhhsecret
  no ip bootp server
  ip domain-name net.galaxy
  ip name-server 220.144.159.1
  ip name-server 220.144.159.2
  ip name-server 219.10.2.1

  !
```

ip telnet source-interface

To specify the IP address of an interface as the source address for Telnet connections, use the `ip telnet source-interface` command in global configuration mode. To reset the source address to the default for each connection, use the `no` form of this command.

```
ip telnet source-interface interface
no ip telnet source-interface
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The interface whose address is to be used as the source for Telnet connections.</td>
</tr>
</tbody>
</table>

**Command Default**
The address of the closest interface to the destination is the source address.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to set the IP address of an interface as the source for all Telnet connections.

If the specified interface is not up, the Cisco IOS software selects the address of the interface closest to the destination as the source address.

**Examples**
The following example forces the IP address for Ethernet interface 1 as the source address for Telnet connections:

```
Router(config)# ip telnet source-interface Ethernet1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip radius source-interface</code></td>
<td>Forwards RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.</td>
</tr>
</tbody>
</table>

ip tftp blocksize

To negotiate a transfer TFTP blocksize, use the `ip tftp blocksize` command in global configuration mode. To disable this configuration, use the `no` form of this command.

```
ip tftp blocksize bytes
```
no ip tftp blocksize

**Syntax Description**

*bytes* | Size of the TFTP block, in bytes. The range is from 512 to 8192.

**Command Default**

The default TFTP blocksize is 512 bytes.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2S</td>
<td>This command was introduced for the 12.2S releases.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into the 15.1(1)SG releases.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3SE</td>
<td>This command was integrated into the Cisco IOS XE Release 3.3SE releases.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set a 1024 byte TFTP blocksize:

```
Router> enable
Router# configure terminal
Router(config)# ip tftp bblocksize 1024
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tftp min-timeout</td>
<td>Specifies the minimum timeout period for retransmission of data.</td>
</tr>
</tbody>
</table>

**ip tftp boot-interface**

To use an interface for TFTP booting, use the `ip tftp boot-interface` command in global configuration mode. To disable this configuration, use the `no` form of this command.

```
ip tftp boot-interface type number
no ip tftp boot-interface
```

**Syntax Description**

*type* | The type of the interface to be used. You can choose from a list of interfaces.

*number* | The related interface number. Each interface has a related range of numbers. For example, the Virtual Multipoint Interface has a range of interface numbers from 1 to 2147483647.

**Command Default**

No interface is used for TFTP booting.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(1)M.</td>
</tr>
</tbody>
</table>
ip tftp min-timeout

To specify the minimum timeout period for retransmission of data using TFTP, use the `ip tftp min-timeout` command in global configuration mode. To disable, use the `no` form of this command.

```
ip tftp min-timeout seconds
no ip tftp min-timeout
```

**Syntax Description**

- `seconds` Specifies the timeout value, in seconds. The range is from 4 to 20.

**Command Default**

The default minimum timeout period for retransmission of data is 4 seconds.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify the minimum timeout period for retransmission of data as 5 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip tftp min-timeout 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tftp boot-interface</td>
<td>Ensures that an interface is used for TFTP booting.</td>
</tr>
</tbody>
</table>
no ip tftp source-interface

**Syntax Description**

| interface-type interface-number | The interface type and number whose address is to be used as the source for TFTP connections. |

**Command Default**

The address of the closest interface to the destination is selected as the source address.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(6)</td>
<td>Destination address lookup in a Virtual Private Network (VPN) routing and forwarding (VRF) table was added for the transfer of TFTP packets.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(8)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set the IP address of an interface as the source for all TFTP connections.

If the specified interface is not up, the Cisco IOS software selects the address of the interface closest to the destination as the source address.

In Cisco IOS 12.3(6) and later releases, TFTP is VRF-aware, which means that TFTP transfer is supported across an interface within a Virtual Private Network (VPN) routing and forwarding (VRF) instance. To specify a VRF as a source for TFTP connections, the VRF must be associated with the same interface that you configure with the `ip tftp source-interface` command. In this configuration, TFTP looks for the destination IP address for file transfer in the specified VRF table.

**Examples**

The following example shows how to configure the router to use the IP address associated with loopback interface 0 as the source address for TFTP connections:

```
Router# configure terminal
Router(config)# ip tftp source-interface loopback0
```

The following example shows how to configure the router to use the VRF table named vpn1 to look for the destination IP address for TFTP connections. In this example, file transfer using TFTP is accomplished across an interface within a VRF (VRF vpn1) link.

```
Router# configure terminal
Router(config)# ip tftp source-interface ethernet 1/0
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target both 100:1
Router(config-vrf)# interface ethernet 1/0
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# end
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ftp source-interface</strong></td>
<td>Forces outgoing FTP packets to use the IP address of a specified interface as the source address.</td>
</tr>
<tr>
<td><strong>ip radius source-interface</strong></td>
<td>Forces outgoing RADIUS packets to use the IP address of a specified interface as the source address.</td>
</tr>
</tbody>
</table>

### ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

**ip wccp web-cache accelerated**

Between brackets, you can use:

- group-address **group-address** *(Optional)* Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the “Usage Guidelines” section for additional information.
- redirect-list **access-list** *(Optional)* Directs the router to use an access list to control traffic that is redirected to this service group. See the “Usage Guidelines” section for additional information.
- group-list **access-list** *(Optional)* Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the “Usage Guidelines” section for additional information.
- password **password** *(Optional)* Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the “Usage Guidelines” section for additional information.

### Command Default

When this command is not configured, hardware acceleration for WCCPv1 is not enabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXD1</td>
<td>This command was changed to support the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **group-address** **group-address** option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received.
on this group address. In addition, the response is sent to the group address. The default is for no `group-address` to be configured, so that all “Here I Am” messages are responded to with a unicast reply.

The `redirect-list access-list` option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The `access-list` argument specifies either a number from 1 to 99 to represent a standard or extended access list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no `redirect-list` to be configured (all traffic is redirected).

The `group-list access-list` option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The `access-list` argument specifies either a number from 1 to 99 to represent a standard access list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no `group-list` to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

### Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip wccp version</code></td>
<td>Specifies which version of WCCP to configure on your router.</td>
</tr>
</tbody>
</table>
L through mode

• L through mode, on page 248
L through mode

length

To set the terminal screen length, use the `length` command in line configuration mode. To restore the default value, use the `no` form of this command.

```
length  screen-length
no  length
```

**Syntax Description**

| screen-length | The number of lines on the screen. A value of zero disables pausing between screens of output. |

**Command Default**

Screen length of 24 lines

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Cisco IOS software uses the value of this command to determine when to pause during multiple-screen output. Not all commands recognize the configured screen length. For example, the `show terminal` command assumes a screen length of 24 lines or more.

**Examples**

In the following example, the terminal type is specified and the screen pause function is disabled for the terminal connection on line 6:

```
Router(config)# line 6
Router(config-line)# terminal-type VT220
Router(config-line)# length 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>terminal length</code></td>
<td>Sets the number of lines on the current terminal screen for the current session.</td>
</tr>
</tbody>
</table>

load-interval

To change the length of time for which data is used to compute load statistics, use the `load-interval` command in interface configuration, Frame Relay DLCI configuration, or template configuration modes. To revert to the default setting, use the `no` form of this command.

```
load-interval  seconds
```
**no load-interval seconds**

**Syntax Description**

| seconds | Length of time for which data is used to compute load statistics. Value is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on). The default is 300 seconds. |

**Command Default**

Enabled

**Command Modes**

Interface configuration

Frame Relay DLCI configuration

Template configuration (config-template)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>This command was made available in Frame Relay DLCI configuration mode.</td>
</tr>
<tr>
<td>12.2(18)SXF</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.1(2)SNG</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>15.2(2)E</td>
<td>This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.6E</td>
<td>This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To make computations more reactive to short bursts of traffic, you can shorten the length of time over which load averages are computed.

If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including the input rate in bits and packets per second, the output rate in bits and packets per second, the load, and reliability.

Load data is gathered every five seconds. This data is used for a weighted-average calculation in which recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data.

If you change the calculation interval from the default of five minutes to a shorter period of time, the input and output statistics that are displayed by the `show interface` command or the `show frame-relay pvc` command will be more current and will be based on more nearly instantaneous data, rather than reflecting the average load over a longer period of time.

This command is often used for dial backup purposes to increase or decrease the likelihood of implementation of a backup interface, but it can be used on any interface.
Examples

**Interface Example**

In the following example, the default average of five minutes is changed to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default five-minute interval might trigger a dial backup for this interface, which is set for the shorter 30-second interval.

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

**Frame Relay PVC Example**

In the following example, the load interval is set to 60 seconds for a Frame Relay PVC with the DLCI 100:

```
Router(config)# interface serial 1/1
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# load-interval 60
```

**Interface Template Example**

In the following example, the load interval is set to 60 seconds in an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# load-interval 60
Device(config-template)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces</code></td>
<td>Displays statistics for all interfaces configured on the router or access server.</td>
</tr>
</tbody>
</table>

### location

To provide a description of the location of a serial device, use the `location` command in line configuration mode. To remove the description, use the `no` form of this command.

```
location text
no location
```

#### Syntax Description

<table>
<thead>
<tr>
<th><strong>text</strong></th>
<th>Location description.</th>
</tr>
</thead>
</table>

#### Command Default

A location description is not provided.

#### Command Modes

Line configuration (config-line)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SR</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SR.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `location` command enters information about the device location and status. Use the `show users all` EXEC command to display the location information.

Examples

In the following example, the location description for the console line is given as “Building 3, Basement”:

```
Router(config)# line console
Router(config-line)# location Building 3, Basement
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show users</code></td>
<td>Displays information about the active lines on a router.</td>
</tr>
</tbody>
</table>

**lock**

To configure a temporary password on a line, use the `lock` command in EXEC mode.

```
lock
```

Syntax Description

This command has no arguments or keywords.

Command Default

Not locked

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced in a release prior to Cisco IOS Release 10.0.</td>
</tr>
<tr>
<td>12.2(33)SR</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SR.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can prevent access to your session while keeping your connection open by setting up a temporary password. To lock access to the terminal, perform the following steps:

1. Enter the `lock` command. The system prompts you for a password.
2. Enter a password, which can be any arbitrary string. The system will prompt you to confirm the password. The screen then clears and displays the message “Locked.”
3. To regain access to your sessions, reenter the password.
The Cisco IOS software honors session timeouts on a locked lines. You must clear the line to remove this feature. The system administrator must set the line up to allow use of the temporary locking feature by using the `lockable` line configuration command.

### Examples

The following example shows configuring the router as lockable, saving the configuration, and then locking the current session for the user:

```
Router(config-line)# lockable
Router(config-line)# ^Z
Router# copy system:running-config nvram:startup-config
Building configuration...
OK
Router# lock
Password: <password>
Again: <password>
Locked
Password: <password>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lockable</td>
<td>Enables the lock EXEC command.</td>
</tr>
<tr>
<td>login (EXEC)</td>
<td>Enables or changes a login username.</td>
</tr>
</tbody>
</table>

### lockable

To enable use of the lock EXEC command, use the `lockable` command in line configuration mode. To reinstate the default (the terminal session cannot be locked), use the `no` form of this command.

```
lockable
no lockable
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

Sessions on the line are not lockable (the lock EXEC command has no effect).

#### Command Modes

Line configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

This command enables use of temporary terminal locking, which is executed using the lock EXEC command. Terminal locking allows a user keep the current session open while preventing access by other users.
Examples

In the following example, the terminal connection is configured as lockable, then the current connection is locked:

```
Router# configure terminal
Router(config)# line console 0
Router(config-line)# lockable
Router(config)# ^Z
Router# lock
Password: <password>
Again: <password>
Locked
Password: <password>
Router#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lock</td>
<td>Prevents access to your session by other users by setting a temporary password on your terminal line.</td>
</tr>
</tbody>
</table>

log config

To enter configuration change logger configuration mode, use the `log config` command in archive configuration mode.

```
log config
```

Syntax Description

This command has no arguments or keywords.

Command Default

Configuration change logger configuration mode is not entered.

Command Modes

Archive configuration (config-archive)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to place the device in configuration change logger configuration mode:
Device# configure terminal
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td>hidekeys</td>
<td>Suppresses the display of password information in configuration log files.</td>
</tr>
<tr>
<td>logging enable</td>
<td>Enables the logging of configuration changes.</td>
</tr>
<tr>
<td>logging size</td>
<td>Specifies the maximum number of entries retained in the configuration log.</td>
</tr>
<tr>
<td>notify syslog</td>
<td>Enables the sending of notifications of configuration changes to a remote syslog.</td>
</tr>
<tr>
<td>show archive log config</td>
<td>Displays entries from the configuration log.</td>
</tr>
</tbody>
</table>

### logging buffered

To enable system message logging to a local buffer, use the `logging buffered` command in global configuration mode. To cancel the use of the buffer, use the `no` form of this command. To return the buffer size to its default value, use the `default` form of this command.

```
logging buffered [discriminator discriminator-name] [buffer-size] [severity-level]
o logging buffered
default logging buffered
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discriminator</td>
<td>(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.</td>
</tr>
<tr>
<td>discriminator-name</td>
<td>(Optional) String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.</td>
</tr>
<tr>
<td>buffer-size</td>
<td>(Optional) Size of the buffer, in bytes. The range is 4096 to 2147483647. The default size varies by platform.</td>
</tr>
</tbody>
</table>
**severity-level**  
(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword):

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><code>emergencies</code></td>
</tr>
<tr>
<td>1</td>
<td><code>alerts</code></td>
</tr>
<tr>
<td>2</td>
<td><code>critical</code></td>
</tr>
<tr>
<td>3</td>
<td><code>errors</code></td>
</tr>
<tr>
<td>4</td>
<td><code>warnings</code></td>
</tr>
<tr>
<td>5</td>
<td><code>notifications</code></td>
</tr>
<tr>
<td>6</td>
<td><code>informational</code></td>
</tr>
<tr>
<td>7</td>
<td><code>debugging</code></td>
</tr>
</tbody>
</table>

The default logging level varies by platform but is generally 7. Level 7 means that messages at all levels (0-7) are logged to the buffer.

**Note** Every time you set the desired buffer severity level, the buffer size is set to default. Therefore, enter the value for the buffer size after setting the buffer severity level.

---

**Command Default**  
Varies by platform. For most platforms, logging to the buffer is disabled by default.

**Command Modes**  
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1(17)T</td>
<td>The severity-level argument was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>The discriminator keyword and discriminator-name argument were added.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.2(50)SY</td>
<td>This command was integrated into Cisco IOS Release 12.2(50)SY.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command copies logging messages to an internal buffer. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

Specifying a severity-level causes messages at that level and numerically lower levels to be logged in an internal buffer.

The optional discriminator keyword and discriminator-name argument provide another layer of filtering that you can use to control the type and number of syslog messages that you want to receive.
When you resize the logging buffer, the existing buffer is freed and a new buffer is allocated. To prevent the router from running out of memory, do not make the buffer size too large. You can use the `show memory` EXEC command to view the free processor memory on the router; however, the memory value shown is the maximum available and should not be approached. The `default logging buffered` command resets the buffer size to the default for the platform.

On Catalyst 6500 standalone switches and Catalyst 6500 virtual switches, the default logging buffered size is 8192.

To display messages that are logged in the buffer, use the `show logging` command. The first message displayed is the oldest message in the buffer.

The `show logging` command displays the addresses and levels associated with the current logging setup and other logging statistics.

The table below shows a list of levels and corresponding syslog definitions.

<table>
<thead>
<tr>
<th>Level</th>
<th>Level Keyword</th>
<th>Syslog Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>emergencies</td>
<td>LOG_EMERG</td>
</tr>
<tr>
<td>1</td>
<td>alerts</td>
<td>LOG_ALERT</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
<td>LOG_CRIT</td>
</tr>
<tr>
<td>3</td>
<td>errors</td>
<td>LOG_ERR</td>
</tr>
<tr>
<td>4</td>
<td>warnings</td>
<td>LOG_WARNING</td>
</tr>
<tr>
<td>5</td>
<td>notifications</td>
<td>LOG_NOTICE</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
<td>LOG_INFO</td>
</tr>
<tr>
<td>7</td>
<td>debugging</td>
<td>LOG_DEBUG</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

The following example shows how to use a message discriminator named buffer1 to filter critical messages, meaning that messages at levels 0, 1, and 2 are filtered:

```
Router(config)# logging buffered discriminator buffer1 critical
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging</td>
<td>Clears messages from the logging buffer.</td>
</tr>
</tbody>
</table>
logging buginf

To allow debug messages to be generated for the standard system logging buffer, use the **logging buginf** command in global configuration mode. To disable the logging for debugging functionality, use the **no** form of this command.

**logging buginf**

**no logging buginf**

**Syntax Description**  
This command has no arguments or keywords.

**Command Default**  
Debug messages are not suppressed.

**Command Modes**  
Global configuration (config)

**Command History**  

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  
The **no logging buginf** command is used to avoid a situation where a large amount of debug messages might overload the processor (CPU hog condition). This condition differs from the use of the **undebug all** command wherein all debugging calls are disabled in the Cisco IOS software. No debug reporting is available, even if debugging is enabled. Note that even though debugging has been completely disabled in the system, other message reporting, including error reporting, is still available.

**Examples**  
The following example shows how to enable buginf logging for debugging:

```
Router# configure terminal
Router(config)# logging buginf
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>Displays the state of system logging (syslog) and the contents of the standard system logging buffer.</td>
</tr>
</tbody>
</table>

**logging enable**

To enable the logging of configuration changes, use the `logging enable` command in configuration change logger configuration mode. To disable the logging of configuration changes, use the `no` form of this command.

```
logging enable
no logging enable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Configuration change logging is disabled.

**Command Modes**

Configuration change logger configuration (config-archive-log-config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command if you want to log configuration changes. If you disable configuration logging, all configuration log records that were collected are purged.

**Examples**

The following example shows how to enable configuration logging:

```
Device# configure terminal
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# logging enable
Device(config-archive-log-config)# end
```

The following example shows how to clear the configuration log by disabling and then reenabling the configuration log:

```
Device# configure terminal
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td>hidekeys</td>
<td>Suppresses the display of password information in configuration log files.</td>
</tr>
<tr>
<td>log config</td>
<td>Enters configuration change logger configuration mode.</td>
</tr>
<tr>
<td>logging size</td>
<td>Specifies the maximum number of entries retained in the configuration log.</td>
</tr>
<tr>
<td>notify syslog</td>
<td>Enables the sending of notifications of configuration changes to a remote syslog.</td>
</tr>
<tr>
<td>show archive log config</td>
<td>Displays entries from the configuration log.</td>
</tr>
</tbody>
</table>

logging esm config

To permit configuration changes from Embedded Syslog Manager (ESM) filters, use the `logging esm config` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
logging esm config
no logging esm config
```

Syntax Description

This command has no arguments or keywords.

Command Default

ESM filters are enabled.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can use the `no logging esm config` command to disallow configuration changes from ESM filters.

Examples

The following example shows how to configure the ESM filters:
Router# configure terminal
Router(config)# logging esm config

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging filter</td>
<td>Specifies a syslog filter module to be used by the ESM.</td>
</tr>
</tbody>
</table>

logging event bundle-status

To enable message bundling, use the `logging event bundle-status` command in interface configuration mode. To disable message bundling, use the `no` form of this command.

```
logging event bundle-status
no logging event bundle-status
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enables system logging of interface state-change events on all interfaces in the system.</td>
</tr>
<tr>
<td>boot</td>
<td>Enables system logging of interface state-change events on all interfaces in the system during system initialization.</td>
</tr>
</tbody>
</table>

Command Default

Message bundling does not occur.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The logging event bundle-status command is not applicable on Port Channel or Ether-Channel interfaces.

Examples

This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:

```
Router(config)# logging event bundle-status
Router(config)# end
Router # show logging event bundle-status
*Aug 4 17:36:48.240 UTC: %EC-SP-5-UNBUNDLE: Interface FastEthernet9/23 left the port-channel Port-channel12
*Aug 4 17:36:48.256 UTC: %LINK-SP-5-CHANGED: Interface FastEthernet9/23, changed state to administratively down
*Aug 4 17:36:47.865 UTC: %EC-SPSTBY-5-UNBUNDLE: Interface FastEthernet9/23 left the port-channel Port-channel12
Router # show logging event bundle-status
*Aug 4 17:37:35.845 UTC: %EC-SP-5-BUNDLE: Interface FastEthernet9/23 joined port-channel Port-channel12
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>

logging event link-status (global configuration)

To change the default or set the link-status event messaging during system initialization, use the logging event link-status command in global configuration mode. To disable the link-status event messaging, use the no form of this command.

logging event link-status {default|boot}
no logging event link-status {default|boot}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enables system logging of interface state-change events on all interfaces in the system.</td>
</tr>
<tr>
<td>boot</td>
<td>Enables system logging of interface state-change events on all interfaces in the system during system initialization.</td>
</tr>
</tbody>
</table>

Command Default

Interface state-change messages are not sent.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You do not have to enter the logging event link-status boot command to enable link-status messaging during system initialization. The logging event link-status default command logs system messages even during system initialization.

If you enter both the logging event link-status default and the no logging event link-status boot commands, the interface state-change events are logged after all modules in the Cisco 7600 series router come online after system initialization. The logging event link-status default and the no logging event link-status boot commands are saved and retained in the running configuration of the system.

When both the logging event link-status default and the no logging event link-status boot commands are present in the running configuration and you want to display the interface state-change messages during system initialization, enter the logging event link-status boot command.

Examples

This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:
Router(config)# logging event link-status default
Router(config)#
This example shows how to enable the system logging of interface state-change events on all interfaces during system initialization:

Router(config)# logging event link-status boot
Router(config)#
This example shows how to disable the system logging of interface state-change events on all interfaces:

Router(config)# no logging event link-status default
Router(config)#
This example shows how to disable the system logging of interface state-change events during system initialization:

Router(config)# no logging event link-status boot
Router(config)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>

logging event link-status (interface configuration)

To enable link-status event messaging on an interface, use the `logging event link-status` command in interface configuration mode. To disable link-status event messaging, use the `no` form of this command.

```
logging event link-status [{bchan|dchan|nfas}]
no logging event link-status [{bchan|dchan|nfas}]
```

### Syntax Description

- **bchan**: (Optional) Logs B-channel status messages. This keyword is available only for integrated services digital network (ISDN) serial interfaces.
- **dchan**: (Optional) Logs D-channel status messages. This keyword is available only for ISDN serial interfaces.
- **nfas**: (Optional) Logs non-facility associated signaling (NFAS) D-channel status messages. This keyword is available only for ISDN serial interfaces.

### Command Default

Interface state-change messages are not sent.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>
This command was modified to support the Supervisor Engine 2.

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

Usage Guidelines

To enable system logging of interface state-change events on a specific interface, enter the `logging event link-status` command.

Examples

The following example shows how to enable link-status event messaging on an interface:

```
Router(config-if)# logging event link-status
```

This example shows how to disable link-status event messaging on an interface:

```
Router(config-if)# no logging event link-status
```

**logging event subif-link-status**

To enable the link-status event messaging on a subinterface, use the `logging event subif-link-status` command in interface configuration mode. To disable the link-status event messaging on a subinterface, use the `no` form of this command.

```
logging event subif-link-status
no logging event subif-link-status
```

Syntax Description

This command has no arguments or keywords.

Command Default

Subinterface state-change messages are not sent.

Command Modes

Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

To enable system logging of interface state-change events on a specific subinterface, enter the `logging event subif-link-status` command.

To enable system logging of interface state-change events on a specific interface, enter the `logging event link-status` command.

To enable system logging of interface state-change events on all interfaces in the system, enter the `logging event link-status` command.
Examples

This example shows how to enable the system logging of the interface state-change events on a subinterface:

Router(config-if)# logging event subif-link-status
Router(config-if)#

This example shows how to disable the system logging of the interface state-change events on a subinterface:

Router(config-if)# no logging event subif-link-status
Router(config-if)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>

logging event trunk-status

To enable trunk status messaging, use the **logging event trunk-status** command in interface configuration mode. To disable trunk status messaging, use the **no** form of this command.

```
logging event trunk-status
no logging event trunk-status
```

Syntax Description

This command has no keywords or variables.

Command Default

This command has no default settings.

Command Modes

Interface configuration mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The logging event bundle-status command is not applicable on Port Channel or Ether-Channel interfaces.

Examples

This example shows how to enable the trunk status messaging on physical ports:

```
Router(config)# logging event trunk-status
Router(config)# end
Router# show logging event trunk-status
*Aug 4 17:27:01.404 UTC: %DTP-SPSTBY-5-NONTRUNKPORTON: Port Gi3/3 has become non-trunk
*Aug 4 17:27:00.773 UTC: %DTP-SP-5-NONTRUNKPORTON: Port Gi3/3 has become non-trunk
Router#
```
logging reload

To set the reload logging level, use the **logging reload** command in global configuration mode. To disable the reload logging, use the **no** form of this command.

```
logging reload [message-limit number]
[ {severity-level|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings} ]
no logging reload
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message-limit</td>
<td>(Optional) Sets the limit on the number of messages that can be logged during reload.</td>
</tr>
<tr>
<td>number</td>
<td>Number of messages. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td>severity-level</td>
<td>(Optional) Logging severity level. The range is from 0 to 7.</td>
</tr>
<tr>
<td>alerts</td>
<td>(Optional) Specifies that an immediate action is needed.</td>
</tr>
<tr>
<td>critical</td>
<td>(Optional) Specifies the critical conditions.</td>
</tr>
<tr>
<td>debugging</td>
<td>(Optional) Displays the debugging messages</td>
</tr>
<tr>
<td>emergencies</td>
<td>(Optional) Specifies that the system is unusable.</td>
</tr>
<tr>
<td>errors</td>
<td>(Optional) Specifies error conditions</td>
</tr>
<tr>
<td>informational</td>
<td>(Optional) Specifies error informational messages</td>
</tr>
<tr>
<td>notifications</td>
<td>(Optional) Specifies normal but significant conditions.</td>
</tr>
<tr>
<td>warnings</td>
<td>(Optional) Specifies warning conditions.</td>
</tr>
</tbody>
</table>

**Command Default**

The logging reload message limit is 1000 notifications.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release c2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default setting is recommended. Setting the message-limit too low may result in losing important messages during reload. If the **logging reload** command is not enabled, logging is turned off during reload.
The following example shows how to set the limit on number of messages that can be logged during reload to 100:

Router# configure terminal
Router(config)# logging reload message-limit 100

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>Displays the state of system logging (syslog) and the contents of the standard system logging buffer.</td>
</tr>
</tbody>
</table>

**logging ip access-list cache (global configuration)**

To configure the Optimized ACL Logging (OAL) parameters, use the `logging ip access-list cache` command in global configuration mode. To return to the default settings, use the `no` form of this command.

```
logging ip access-list cache {entries entries|interval seconds|rate-limit pps|threshold packets}
```

```
no logging ip access-list cache [{entries|interval|rate-limit|threshold}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>entries entries</th>
<th>Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval seconds</td>
<td>Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.</td>
</tr>
<tr>
<td>rate-limit pps</td>
<td>Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.</td>
</tr>
<tr>
<td>threshold packets</td>
<td>Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.</td>
</tr>
</tbody>
</table>

**Command Default**

The defaults are as follows:

- `entries` -- 8000 entries.
- `seconds` -- 300 seconds (5 minutes).
- `rate-limit` `pps` -- 0 (rate limiting is off) and all packets are logged.
- `threshold` `packets` -- 0 (rate limiting is off) and the system log is not triggered by the number of packet matches.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the `update-interval` seconds command, the entry is removed from the cache.

If you enter the `no logging ip access-list cache` command without keywords, all the parameters are returned to the default values.

You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

When enabling the IP "too short" check using the `mls verify ip length minimum` command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

---

**Caution**

Using optimized access-list logging (OAL) and the `mls verify ip length minimum` command together can cause routing protocol neighbor flapping as they are incompatible.

---

**Examples**

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)#
logging ip access-list cache entries 200
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache interval 350
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)#
logging ip access-list cache rate-limit 100
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache threshold 125
```

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear logging ip access-list cache</code></td>
<td>Clears all the entries from the OAL cache and sends them to the syslog.</td>
</tr>
<tr>
<td><code>logging ip access-list cache (interface configuration)</code></td>
<td>Enables an OAL-logging cache on an interface that is based on direction.</td>
</tr>
</tbody>
</table>
**logging ip access-list cache (interface configuration)**

To enable an Optimized ACL Logging (OAL)-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command in interface configuration mode. To disable OAL, use the **no** form of this command.

```
logging ip access-list cache [{in|out}]
no logging ip access-list cache
```

**Syntax Description**
- `in` (Optional) Enables OAL on ingress packets.
- `out` (Optional) Enables OAL on egress packets.

**Command Default**
Disabled

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

This command is supported on traffic that matches the **log** keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** seconds command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.
Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible.

**Examples**

This example shows how to enable OAL on ingress packets:

```
Router(config-if)#
logging ip access-list cache in
```

This example shows how to enable OAL on egress packets:

```
Router(config-if)#
logging ip access-list cache out
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging ip access-list cache</td>
<td>Clears all the entries from the OAL cache and sends them to the syslog.</td>
</tr>
<tr>
<td>logging ip access-list cache (global configuration)</td>
<td>Configures the OAL parameters.</td>
</tr>
<tr>
<td>show logging ip access-list</td>
<td>Displays information about the logging IP access list.</td>
</tr>
<tr>
<td>update-interval  seconds</td>
<td>Removes entries from the cache that are inactive for the duration that is specified in the command.</td>
</tr>
</tbody>
</table>

### logging persistent (config-archive-log-cfg)

To enable the configuration logging persistent feature and to select how the configuration commands are to be saved to the Cisco IOS secure file system, use the `logging persistent` command in the log config submode of archive configuration mode. To disable this capability, use the `no` form of this command.

```
logging persistent {auto|manual}
no logging persistent {auto|manual}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Specifies that each configuration command will be saved automatically to the Cisco IOS secure file system.</td>
</tr>
<tr>
<td>manual</td>
<td>Specifies that each configuration command must be saved manually to the Cisco IOS secure file system.</td>
</tr>
</tbody>
</table>

**Command Default**

The configuration commands are not saved to the Cisco IOS secure file system.

**Command Modes**

Archive configuration mode, log config (configuration-change logger) submode (config-archive-log-cfg)#
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When you use the manual keyword, you must save each configuration command manually to the Cisco IOS secure file system. To do this, you must use the archive log config persistent save command.

Examples

The following example automatically saves the configuration commands to the Cisco IOS secure file system:

Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-cfg)# logging enable
Router(config-archive-log-cfg)# logging persistent auto

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging persistent reload</td>
<td>Sequentially applies configuration commands in the configuration logger database to the running-config file after a reload.</td>
</tr>
<tr>
<td>archive log config persistent save</td>
<td>Saves the persisted commands in the configuration log to the Cisco IOS secure file system.</td>
</tr>
</tbody>
</table>

logging persistent reload (config-archive-log-cfg)

To sequentially apply the configuration commands saved in the configuration logger database (since the last write memory command) to the running-config file after a reload, use the logging persistent reload command in configuration change logger configuration mode in archive configuration mode. To disable this capability, use the no form of this command.

logging persistent reload
no logging persistent reload

Syntax Description

This command has no arguments or keywords.

Command Default

The configuration commands saved in the configuration logger database are not applied to the running-config file.
**Command Modes**

Archive config mode; log config (configuration change logger) submode (config-archive-log-cfg)##

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `logging persistent reload` command when you want changed configuration commands to take effect on the next reload of the router.

**Examples**

The following example applies the configuration commands in the configuration logger database to the running-config file after the next reload:

```
Router(config-archive-log-cfg)# logging persistent reload
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging persistent</code></td>
<td>Enables the configuration logging persistent feature.</td>
</tr>
</tbody>
</table>

**logging size**

To specify the maximum number of entries retained in the configuration log, use the `logging size` command in configuration change logger configuration mode. To reset the default value, use the `no` form of this command.

```
logging size entries
no logging size
```

**Syntax Description**

`entries` The maximum number of entries retained in the configuration log. Valid values range from 1 to 1000. The default value is 100 entries.

**Command Default**

100 entries

**Command Modes**

Configuration change logger configuration (config-archive-log-config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Cisco IOS Configuration Fundamentals Command Reference
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the configuration log is full, the oldest log entry is removed every time a new entry is added.

**Note**

If a new log size is specified that is smaller than the current log size, the oldest entries will be immediately purged until the new log size is satisfied, regardless of the age of the log entries.

Examples

The following example shows how to specify that the configuration log may have a maximum of 200 entries:

```
Device(config-archive-log-config)# logging size 200
```

The following example shows how to clear the configuration log by reducing the log size to 1, then resetting the log size to the desired value. Only the most recent configuration log file will be saved.

```
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# logging size 1
Device(config-archive-log-config)# logging size 200
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td>hidekeys</td>
<td>Suppresses the display of password information in configuration log files.</td>
</tr>
<tr>
<td>log config</td>
<td>Enters configuration change logger configuration mode.</td>
</tr>
<tr>
<td>logging enable</td>
<td>Enables the logging of configuration changes.</td>
</tr>
<tr>
<td>notify syslog</td>
<td>Enables the sending of notifications of configuration changes to a remote syslog.</td>
</tr>
<tr>
<td>show archive log config</td>
<td>Displays entries from the configuration log.</td>
</tr>
</tbody>
</table>

logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the `logging synchronous` command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the `no` form of this command.

```
logging synchronous [level severity-level|all] [limit number-of-lines]
```
no logging synchronous [ {(level severity-level[all])} [limit number-of-lines] ]

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>level severity-level</td>
<td>(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.</td>
</tr>
<tr>
<td>limit number-of-lines</td>
<td>(Optional) Specifies the number of buffer lines to be queued for the terminal, after which new messages are dropped. The default value is 20.</td>
</tr>
</tbody>
</table>

Command Default

This command is disabled.

If you do not specify a severity level, the default value of 2 is assumed.

If you do not specify the maximum number of buffers to be queued, the default value of 20 is assumed.

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When synchronous logging of unsolicited messages and debug output is turned on, unsolicited Cisco IOS software output is displayed on the console or printed after solicited Cisco IOS software output is displayed or printed. This keeps unsolicited messages and debug output from being interspersed with solicited software output and prompts.

Tip

This command is useful for keeping system messages from interrupting your typing. By default, messages will appear immediately when they are processed by the system, and the CLI cursor will appear at the end of the displayed message. For example, the line “Configured by console from console” may be printed to the screen, interrupting whatever command you are currently typing. The **logging synchronous** command allows you to avoid these potentially annoying interruptions without having to turn off logging to the console entirely.

When this command is enabled, unsolicited messages and debug output are displayed on a separate line than user input. After the unsolicited messages are displayed, the CLI returns to the user prompt.

Note

This command is also useful for allowing you to continue typing when debugging is enabled.

When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity.
When a message queue limit of a terminal line is reached, new messages are dropped from the line, although these messages might be displayed on other lines. If messages are dropped, the notice “%SYS-3-MSGLOST number-of-messages due to overflow” follows any messages that are displayed. This notice is displayed only on the terminal that lost the messages. It is not sent to any other lines, any logging servers, or the logging buffer.

Caution

By configuring abnormally large message queue limits and setting the terminal to “terminal monitor” on a terminal that is accessible to intruders, you expose yourself to “denial of service” attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages could consume all available RAM. You should guard against this type of attack through proper configuration.

Examples

In the following example, a system message appears in the middle of typing the show running-config command:

Router(config-line)# end
Router# show ru
2w1d: %SYS-5-CONFIG_I: Configured from console by consolenning-config
  .
  .

The user then enables synchronous logging for the current line (indicated by the * symbol in the show line command), after which the system displays the system message on a separate line, and returns the user to the prompt to allow the user to finish typing the command on a single line:

Router# show line
    Tty Typ  Tx/Rx  A Modem Roty  Acc0  Acc1  Uses  Noise  Overruns  Int
  *  0 CTY   - - - - - - - 0 3 0/0 -
  .
  .
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# line 0
Router(config-line)# logging syn
      <tab>
Router(config-line)# logging synchronous

Router(config-line)# end
Router# show ru
2w1d: %SYS-5-CONFIG_I: Configured from console by console
Router# show running-config

In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

Router(config)# line 4
Router(config-line)# logging synchronous level 6
Router(config-line)# exit
Router(config)# line 2
Router(config-line)# logging synchronous level 7 limit 1000
Router(config-line)# end
Router#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>Identifies a specific line for configuration and starts the line configuration command collection mode.</td>
</tr>
<tr>
<td>logging on</td>
<td>Controls logging of error messages and sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.</td>
</tr>
</tbody>
</table>

### logging system

To enable System Event Archive (SEA) logging, use the `logging system` command in global configuration mode. To disable SEA logging, use the `no` form of this command.

```plaintext
logging system [disk name]
no logging system
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk name</td>
<td>(Optional) Stores the system event archive (system event log file) in the specified disk. The specified disk must be already have been configured to allow for the storage of the system event archive.</td>
</tr>
</tbody>
</table>

#### Command Default

By default, SEA logging feature is enabled, and the events are logged to a file on a persistent storage device (bootflash: or disk:).

#### Command Modes

Global configuration (config)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>The command was introduced for the Cisco uBR10012 router in the Cisco IOS Software Release 12.2(33)SCC.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

SEA is supported on switches that have a Supervisor Engine 32 or Supervisor Engine 720 with a compact flash adapter and a Compact Flash card (WS-CF-UPG= for Supervisor Engine 720).

To stop SEA logging to a specified disk, use the `default logging system` command.

For documentation of the configuration tasks associated with this feature, see the chapter “Configuring the System Event Archive” in the *Catalyst 6500 Release 12.2SX Software Configuration Guide*.

Cisco Universal Broadband Router 100112
The SEA feature is used to address the deficiencies of the debug trace and system console. Support for SEA feature was introduced on Cisco uBR10012 Router in the Cisco IOS Release 12.2(33)SRA. Use the `logging system disk` command to change the location of the disk used to store the sea_log.dat file.

**Note**
To store the system event logs, the SEA requires either PCMCIA ATA disk or Compact Flash disk in compact flash adapter for PRE2.

**Examples**
The following example shows how to specify that the SEA log file should be written to the disk “disk1”:

```
Router(config)# logging system disk disk1:
Router(config)# end
```

**Related Commands**
- `clear logging system`: Clears the event records stored in the SEA.
- `copy logging system`: Copies the archived system event log to another location.
- `show logging system`: Displays the SEA logging system disk.

**logout**
To close an active terminal session by logging off the router, use the `logout` command in user EXEC mode.

```
logout
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No default behavior or values.

**Command Modes**
User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**
In the following example, the `exit` (global) command is used to move from global configuration mode to privileged EXEC mode, the `disable` command is used to move from privileged EXEC mode to user EXEC mode, and the `logout` command is used to log off (exit from the active session):

```
Router(config)# exit
Router# disable
Router> logout
```
logout-warning

To warn users of an impending forced timeout, use the `logout-warning` command in line configuration mode. To restore the default, use the `no` form of this command.

```
logout-warning [seconds]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Optional</th>
<th>Number of seconds that are counted down before session termination. If no number is specified, the default of 20 seconds is used.</th>
</tr>
</thead>
</table>

**Command Default**

No warning is sent to the user.

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command notifies the user of an impending forced timeout (set using the `absolute-timeout` command).

**Examples**

In the following example, a logout warning is configured on line 5 with a countdown value of 30 seconds:

```
Router(config)# line 5
Router(config-line)# logout-warning 30
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>absolute-timeout</code></td>
<td>Sets the interval for closing user connections on a specific line or port.</td>
</tr>
<tr>
<td><code>session-timeout</code></td>
<td>Sets the interval for closing the connection when there is no input or output traffic.</td>
</tr>
</tbody>
</table>

macro (global configuration)

To create a global command macro, use the `macro` command in global configuration mode. To remove the macro, use the `no` form of this command.

```
```
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>global</code></td>
<td>Applies the macro globally.</td>
</tr>
<tr>
<td><code>apply macro-name</code></td>
<td>Applies a specified macro.</td>
</tr>
<tr>
<td><code>description text</code></td>
<td>Provides a description of the macros applied to the switch.</td>
</tr>
<tr>
<td><code>trace macro-name</code></td>
<td>Applies a specified macro with trace enabled.</td>
</tr>
<tr>
<td><code>keyword-to-value</code></td>
<td>(Optional) Keyword to replace with a value.</td>
</tr>
<tr>
<td><code>value-first-keyword</code></td>
<td>Value of the first keyword to replace.</td>
</tr>
<tr>
<td><code>value-second-keyword</code></td>
<td>Value of the second keyword to replace.</td>
</tr>
<tr>
<td><code>value-third-keyword</code></td>
<td>Value of the third keyword to replace.</td>
</tr>
<tr>
<td><code>name macro-name</code></td>
<td>Specifies the name of a macro.</td>
</tr>
</tbody>
</table>

### Command Default

This command has no default setting.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You can enter up to three keyword pairs using the `macro global trace` command.

You can enter the `macro global description` command on the switch stack or on a standalone switch.

Use the `description text` keyword and argument to associate the comment text, or the macro name with a switch. When multiple macros are applied on a switch, the description text is used from the last applied macro. You can verify the global description settings by using the `show parser macro description` command.

To find the syntax or configuration errors, enter the `macro global trace macro-name` command to apply and debug the macro.

To display a list of any keyword-value pairs defined in the macro, enter the `macro global apply macro-name ?` command.

You can delete a global macro-applied configuration on a switch only by entering the `no` version of each command that is in the macro.

Keyword matching is case sensitive.

When a macro is applied on the commands, all matching occurrences of keywords are replaced with the corresponding values.

The `no` form of the `macro name` command deletes only the macro definition. It does not affect the configuration of the interfaces on which the macro is already applied.

### Examples

The following example shows how to apply the macro called snmp to set the hostname address to “test-server” and to set the IP precedence value to 7:
Router(config)# macro global apply snmp ADDRESS test-server VALUE 7

The following example shows how to debug the macro called snmp by using the macro global trace command to find the syntax or configuration errors in the macro when it is applied to a switch:

Router(config)# macro global trace snmp VALUE 7 VALUE 8 VALUE 9
Applying command...`snmp-server enable traps port-security'
Applying command...`snmp-server enable traps linkup'
Applying command...`snmp-server enable traps linkdown'
Applying command...`snmp-server host'
%Error Unknown error.
Applying command...`snmp-server ip precedence 7'
Router(config)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro (interface configuration)</td>
<td>Creates an interface-specific command macro.</td>
</tr>
<tr>
<td>show parser macro</td>
<td>Displays the smart port macros.</td>
</tr>
</tbody>
</table>

**macro (interface configuration)**

To create an interface-specific command macro, use the macro command in interface configuration mode. To remove the macro, use the no form of this command.

```
```

**Syntax Description**

- **apply macro-name**: Applies a specified macro.
- **description text**: Specifies a description about the macros that are applied to the interface.
- **trace macro-name**: Applies a specified macro with trace enabled.
- **keyword-to-value**: (Optional) Keyword to replace with a value.
- **value-first-keyword**: Value of the keyword to replace.

**Command Default**

This command has no default setting.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can enter up to three keyword changes using the macro trace command.

You can enter the macro description command on the switch stack or on a standalone switch.
Use the description text keyword and argument to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro. You can verify the description settings by entering the show parser macro description command.

To find any syntax or configuration errors, enter the macro trace macro-name command to apply and debug the macro.

To display a list of any keyword-value pairs defined in the macro, enter the macro apply macro-name ? command.

To successfully apply the macro, you must enter any required keyword-value pairs.

Keyword matching is case sensitive.

In the commands that the macro applies, all matching occurrences of keywords are replaced with the corresponding values.

You can delete all configuration on an interface by entering the default interface interface configuration command.

Examples

The following example shows how to apply the user-created macro called desktop-config and to verify the configuration:

Router(config)# interface fastethernet1/2
Router(config-if)# macro apply desktop-config

The following example shows how to apply the user-created macro called desktop-config and to replace all occurrences of vlan with VLAN ID 25:

Router(config-if)# macro apply desktop-config vlan 25

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro (global configuration)</td>
<td>Creates a command macro.</td>
</tr>
<tr>
<td>show parser macro</td>
<td>Displays the smart port macros.</td>
</tr>
</tbody>
</table>

maximum

To set the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive, use the maximum command in archive configuration mode. To reset this command to its default, use the no form of this command.

maximum number

no maximum number

Syntax Description

| number | Maximum number of archive files of the running configuration to be saved in the Cisco configuration archive. You can archive from 1 to 14 configuration files. The default is 10. |
By default, a maximum of 10 archive files of the running configuration are saved in the Cisco configuration archive.

**Command Modes**

Archive configuration (config-archive)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, you must configure the path command to specify the location and filename prefix for the files in the Cisco configuration archive.

After the maximum number of files are saved in the Cisco configuration archive, the oldest file is automatically deleted when the next, most recent file is saved.

This command should only be used when a local writable file system is specified in the url argument of the path command. Network file systems may not support deletion of previously saved files.

**Examples**

In the following example, a value of 5 is set as the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive:

```plaintext
configure terminal
! archive
path disk0:myconfig
maximum 5
end
```
memory cache error-recovery

To trace error recovery in memory using caches, use the `memory cache error-recovery` command in global configuration mode. To disable the memory cache error recovery mechanisms, use the `no` form of this command.

```
memory cache error-recovery {L1|L2|L3} {data|inst}
no memory cache error-recovery {L1|L2|L3} {data|inst}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1</td>
<td>Specifies the L1 cache.</td>
</tr>
<tr>
<td>L.2</td>
<td>Specifies the L2 cache.</td>
</tr>
<tr>
<td>L.3</td>
<td>Specifies the L3 cache.</td>
</tr>
<tr>
<td>data</td>
<td>Specifies if data recovery is required.</td>
</tr>
<tr>
<td>inst</td>
<td>Specifies if instruction recovery is required.</td>
</tr>
</tbody>
</table>

### Command Default

Memory cache error recovery mechanisms are not enabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable the `memory cache error-recovery` command:

```
Router> enable
Router# configure terminal
Router(config)# memory cache error-recovery
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory cache error-recovery options</td>
<td>Traces error recovery in memory using caches through set options.</td>
</tr>
</tbody>
</table>

memory cache error-recovery options

To trace error recovery in memory using caches through set options, use the `memory cache error-recovery options` command in global configuration mode. To disable the set memory cache error recovery mechanisms, use the `no` form of this command.

```
memory cache error-recovery options {abort-if-same-content|blocking-mode|max-recoveries value|nvram-report|parity-check|window seconds}
```

```
no memory cache error-recovery options {abort-if-same-content|blocking-mode|max-recoveries value|nvram-report|parity-check|window seconds}
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abort-if-same-content</td>
<td>Abort recovery if the cache contains the same content as the memory.</td>
</tr>
<tr>
<td>blocking-mode</td>
<td>Sets the memory blocking mode to special or ON.</td>
</tr>
<tr>
<td>max-recoveries value</td>
<td>The maximum number of recoveries allowed within a time window. Specify a value in the range 0 to 255.</td>
</tr>
<tr>
<td>nvram-report</td>
<td>Saves the report in the NVRAM.</td>
</tr>
<tr>
<td>parity-check</td>
<td>Sets the parity checking mode to normal or ON.</td>
</tr>
<tr>
<td>window seconds</td>
<td>The time window, in seconds. Specify a value in the range 1 to 3153600.</td>
</tr>
</tbody>
</table>

Command Default

Memory cache error recovery mechanisms are not enabled.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enable the `memory cache error-recovery options` command:

```
Router> enable
Router# configure terminal
Router(config)# memory cache error-recovery options abort-if-same-content
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory cache error-recovery</td>
<td>Traces error recovery in memory using caches.</td>
</tr>
</tbody>
</table>
**memory free low-watermark**

To configure a router to issue system logging message notifications when available memory falls below a specified threshold, use the `memory free low-watermark` command in global configuration mode. To disable memory threshold notifications, use the `no` form of this command.

```
memory free low-watermark {processor threshold|io threshold}
no memory free low-watermark
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>processor</code></td>
<td>Sets the processor memory threshold in kilobytes. When available processor memory falls below this threshold, a notification message is triggered. Valid values are 1 to 4294967295.</td>
</tr>
<tr>
<td><code>io</code></td>
<td>Sets the input/output (I/O) memory threshold in kilobytes. When available I/O memory falls below this threshold, a notification message is triggered. Valid values are 1 to 4294967295.</td>
</tr>
</tbody>
</table>

### Command Default

Memory threshold notifications are disabled.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Using this command, you can configure a router to issue a system logging message each time available free memory falls below a specified threshold ("low-watermark"). Once available free memory rises to 5 percent above the threshold, another notification message is generated.

### Examples

The following example specifies a free processor memory notification threshold of 20000 KB:

```
Router(config)# memory free low-watermark processor 20000
```

If available free processor memory falls below this threshold, the router sends a notification message like this one:

```
000029: *Aug 12 22:31:19.559: %SYS-4-FREEMENLOW: Free Memory has dropped below 20000k
Pool: Processor Free: 66814056 freemem_lwm: 204800000
```

Once available free processor memory rises to a point 5 percent above the threshold, another notification message like this is sent:
memory lite

To enable the memory allocation lite (malloc_lite) feature, use the `memory lite` command in global configuration mode. To disable this feature, use the `no` form of this command.

```
memory lite
no memory lite
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

This command is enabled by default.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The malloc_lite feature was implemented to avoid excessive memory allocation overhead for situations where less than 128 bytes were required. This feature is supported for processor memory pools only.

The malloc_lite feature is enabled by default. If the malloc_lite feature is disabled using the `no memory lite` command, you can re-enable the feature by entering the `memory lite` command.

### Examples

The following example shows how to disable the malloc_lite feature:

```
no memory lite
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scheduler heapcheck process</code></td>
<td>Performs a “sanity check” for corruption in memory blocks when a process switch occurs.</td>
</tr>
</tbody>
</table>

memory reserve

To reserve a specified amount of memory in kilobytes for console access and critical notifications, use the `memory reserve` command in global configuration mode. To disable the configuration, use the `no` form of this command.
Syntax for Releases 15.0(1)M and 12.2(33)SRC and Later Releases
memory reserve {console size|critical} [total-size]
no memory reserve {console|critical}

Syntax for Releases 12.2(33)SXI, Cisco IOS XE Release 2.1 and Later Releases
memory reserve critical [total-size]
no memory reserve critical

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console size</td>
<td>Reserves the memory size for a console session.</td>
</tr>
<tr>
<td>size</td>
<td>Amount of memory to be reserved, in kilobytes.</td>
</tr>
<tr>
<td>critical</td>
<td>Reserves the memory for critical notifications.</td>
</tr>
<tr>
<td>total-size</td>
<td>(Optional) Total amount of memory to be reserved, in kilobytes. The range is from 0 to 4294967295.</td>
</tr>
</tbody>
</table>

Command Modes

- Global configuration (config)

Command Default

- 256 KB is reserved for console memory access. 100 KB is reserved for critical memory access.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The `memory reserve console` command reserves enough memory to ensure console access to a Cisco IOS device for administrative and troubleshooting purposes. This feature is especially beneficial when the device runs low on memory.

- The `memory reserve critical` command reserves the specified amount of memory in kilobytes so that the router can issue critical notifications. The amount of memory reserved for critical notifications cannot exceed 25 percent of the total available memory.

Examples

- The following example shows how to reserve a specified amount of memory in kilobytes for console access:

  ```
  Router# configure terminal
  Router(config)# memory reserve console 2
  ```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>memory free low-watermark</code></td>
<td>Configures a router to issue system logging message notifications when available memory falls below a specified threshold.</td>
</tr>
</tbody>
</table>

## memory reserve critical

**Note**

Effective with Cisco IOS Release 12.4(15)T1, the `memory reserve critical` command is replaced by the `memory reserve` command. See the `memory reserve` command for more information.

To configure the size of the memory region to be used for critical notifications (system logging messages), use the `memory reserve critical` command in global configuration mode. To disable the reservation of memory for critical notifications, use the `no` form of this command.

```
memory reserve critical kilobytes

no memory reserve critical
```

### Syntax Description

| `kilobytes` | Specifies the amount of memory to be reserved in kilobytes. Valid values are 1 to 4294967295, but the value you specify cannot exceed 25 percent of total memory. The default is 100 kilobytes. |

### Command Default

100 kilobytes of memory is reserved for the logging process.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(15)T1</td>
<td>This command was replaced by the <code>memory reserve</code> command.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command reserves a region of memory on the router so that, when system resources are overloaded, the router retains enough memory to issue critical system logging messages.

**Note**

Once the size of the reserved memory region is specified, any change to the specified value takes effect only after the current configuration is saved and the system has been reloaded.
Examples

The following example shows how to reserve 1,000 KB of system memory for logging messages at the next system restart:

```
Router(config)# memory reserve critical 1000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory free low-watermark</td>
<td>Configures a router to issue syslog notifications when available memory falls below a specified threshold.</td>
</tr>
</tbody>
</table>

memory sanity

To perform a “sanity check” for corruption in buffers and queues, use the `memory sanity` command in global configuration mode. To disable this feature, use the `no` form of this command.

```
memory sanity [buffer|queue|all]
no memory sanity
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer</td>
<td>(Optional) Specifies checking all buffers.</td>
</tr>
<tr>
<td>queue</td>
<td>(Optional) Specifies checking all queues.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Specifies checking all buffers and queues.</td>
</tr>
</tbody>
</table>

Command Default

This command is not enabled by default. If the `buffer` or `queue` keyword is not specified, a sanity check will be performed on all buffers and queues.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the `memory sanity buffer` command is enabled, a sanity check is performed on buffers when a packet buffer is allocated or when a packet buffer is returned to the buffer pool. This command also time-stamps the buffer, which may be useful when tracking the age of a buffer.

The `memory sanity` command can be saved in the startup configuration file and, therefore, it is not necessary to reconfigure this command each time the router is reloaded. Like the `scheduler heapcheck process memory` command, the `memory sanity` command can check for corruption in the I/O memory block.

Enabling the `memory sanity` command may result in slight router performance degradation.

Examples

The following example shows how to perform a sanity check for corruption in all buffers and queues:

```
memory sanity all
```
memory scan

To enable the Memory Scan feature, use the `memory scan` command in global configuration mode. To restore the router configuration to the default, use the `no memory scan` command.

### Syntax Description
This command has no arguments or keywords.

### Command Default
This command is disabled by default.

### Command Modes
Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(4)XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>This command was integrated in Cisco IOS Release 12.0 T for the Cisco 7500 series only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
The Memory Scan feature adds a low-priority background process that searches all installed dynamic random-access memory (DRAM) for possible parity errors. If errors are found in memory areas that are not in use, this feature attempts to scrub (remove) the errors. The time to complete one memory scan and scrub cycle can range from 10 minutes to several hours, depending on the amount of installed memory. The impact of the Memory Scan feature on the central processing unit (CPU) is minimal. To view the status of the memory scan feature on your router, use the `show memory scan` command in EXEC mode.

### Examples
The following example enables the Memory Scan feature on a Cisco 7500 series router:

```
Router(config) # memory scan
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show memory scan</code></td>
<td>Displays the number and type of parity errors on your system.</td>
</tr>
</tbody>
</table>

---

**memory-size iomem**

To reallocate the percentage of DRAM to use for I/O memory and processor memory, use the `memory-size iomem` command in global configuration mode. To revert to the default memory allocation, use the `no` form of this command.

---
**Syntax Description**

- `i/o-memory-percentage`  

  The percentage of DRAM allocated to I/O memory, in bytes. The values permitted are 5, 10, 15, 20, 25, 30, 40, and 50. A minimum of 4 MB of memory is required for I/O memory.

**Command Default**

The default memory allocation is 25 percent of the DRAM to I/O memory and 75 percent of the DRAM to processor memory.

**Note**

If the `smartinit` process has been enabled, the default memory allocation of 25 percent to the I/O memory does not apply. Instead, `smartinit` examines the network modules, and then calculates the memory allocation for the I/O memory.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(15)T1</td>
<td>This command was integrated into Cisco IOS Release 12.4(15)T1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you specify the percentage of I/O memory in the command line, the processor memory automatically acquires the remaining percentage of the DRAM memory.

**Examples**

The following example allocates 40 percent of the DRAM memory to I/O memory and the remaining 60 percent to the processor memory:

```
Router# configure terminal
Router(config)#
memory-size iomem 40
```

Smart-init will be disabled and new I/O memory size will take effect upon reload.

---

**menu (EXEC)**

To display a preconfigured user menu, use the `menu` command in user EXEC or privileged EXEC mode.

```
menu menu-name
```

**Syntax Description**

- `menu-name`  

  The name of the menu.

**Command Modes**

User EXEC
Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A user menu is a type of user interface where text descriptions of actions to be performed are displayed to the user. The user can use the menu to select services and functions without having to know the details of command-line interface (CLI) commands.

Menus can be created for users in global configuration mode, using the commands listed in the “Related Commands” section.

A menu can be invoked at either the user or privileged EXEC level, but if an item in the menu contains a privileged EXEC command, the user must be logged in at the privileged level for the command to succeed.

### Examples

The following example invokes a menu named OnRamp:

```
Router> menu OnRamp
Welcome to OnRamp Internet Services
Type a number to select an option; Type 9 to exit the menu.
1 Read email
2 UNIX Internet access
3 Resume UNIX connection
6 Resume next connection
9 Exit menu system
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu clear-screen</td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user interface menus.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an option number.</td>
</tr>
<tr>
<td>menu options</td>
<td>Sets options for items in user interface menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user interface menu.</td>
</tr>
<tr>
<td>menu single-space</td>
<td>Displays menu items single-spaced rather than double-spaced.</td>
</tr>
<tr>
<td>menu status-line</td>
<td>Displays a line of status information about the current user at the top of a menu.</td>
</tr>
<tr>
<td>menu text</td>
<td>Specifies the text of a menu item in a user interface menu.</td>
</tr>
<tr>
<td>menu title</td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
<tr>
<td>no menu</td>
<td>Deletes a specified menu from a menu configuration.</td>
</tr>
</tbody>
</table>
**menu menu-name single-space**

To display menu items single-spaced rather than double-spaced, use the `menu <menu-name> single-space` command in global configuration mode.

```
menu menu-name single-space
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>menu-name</code></td>
<td>Name of the menu this command should be applied to.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled for menus with more than nine items; disabled for menus with nine or fewer items.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When more than nine menu items are defined, the menu is displayed single-spaced. To configure the menus with nine or fewer items to display single-spaced, use this command.

**Examples**

In the following example, single-spaced menu items are displayed for the menu named Access1:

```
menu Access1 single-space
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td>menu clear-screen</td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an item.</td>
</tr>
<tr>
<td>menu options</td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td>menu status-line</td>
<td>Displays a line of status information about the current user at the top of a menu.</td>
</tr>
<tr>
<td>menu text</td>
<td>Specifies the text of a menu item in a user menu.</td>
</tr>
<tr>
<td>menu title</td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
</tbody>
</table>
**menu clear-screen**

To clear the terminal screen before displaying a menu, use the `menu clear-screen` command in global configuration mode.

```
menu clear-screen menu-name clear-screen
```

**Syntax Description**

- **menu-name**: Name of the menu this command should be applied to.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command uses a terminal-independent mechanism based on termcap entries defined in the router and the configured terminal type for the user. This command allows the same menu to be used on multiple types of terminals instead of having terminal-specific strings embedded within menu titles. If the termcap entry does not contain a clear string, the menu system enters 24 new lines, causing all existing text to scroll off the top of the terminal screen.

**Examples**

In the following example, the terminal screen is cleared before displaying the menu named Access1:

```
Router(config)# menu Access1 clear-screen
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an item.</td>
</tr>
<tr>
<td>menu options</td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td>menu single-space</td>
<td>Displays menu items single-spaced rather than double-spaced.</td>
</tr>
<tr>
<td>menu status-line</td>
<td>Displays a line of status information about the current user at the top of a menu</td>
</tr>
<tr>
<td>menu text</td>
<td>Specifies the text of a menu item in a user menu.</td>
</tr>
<tr>
<td>menu title</td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
</tbody>
</table>
menu command

To specify underlying commands for user menus, use the menu command command in global configuration mode. To return to default settings, use the no form of this command.

```
menu command menu menu-name command menu-item {command|menu-exit}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu menu-name</td>
<td>Name of the menu. You can specify a maximum of 20 characters.</td>
</tr>
<tr>
<td>command menu-item</td>
<td>Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu entries. When the tenth item is added to the menu, the line-mode and single-space options are activated automatically.</td>
</tr>
<tr>
<td>command</td>
<td>Command to issue when the user selects an item.</td>
</tr>
<tr>
<td>menu-exit</td>
<td>Provides a way for menu users to return to a higher-level menu or exit the menu system.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to assign actions to items in a menu. Use the menu text global configuration command to assign text to items. These commands must use the same menu name and menu selection key.

The menu command command has a special keyword for the command argument, menu-exit, that is available only within menus. It is used to exit a submenu and return to the previous menu level, or to exit the menu altogether and return to the EXEC command prompt.

You can create submenus that are opened by selecting entries in another menu. Use the menu EXEC command as the command for the submenu item.

**Note**

If you nest too many levels of menus, the system prints an error message on the terminal and returns to the previous menu level.

When a menu allows connections (their normal use), the command for an entry activating the connection should contain a resume command, or the line should be configured to prevent users from escaping their
sessions with the escape-char none command. Otherwise, when they escape from a connection and return to the menu, there will be no way to resume the session and it will sit idle until the user logs out.

Specifying the resume command as the action that is performed for a selected menu entry permits a user to resume a named connection or connect using the specified name, if there is no active connection by that name. As an option, you can also supply the connect string needed to connect initially. When you do not supply this connect string, the command uses the specified connection name.

You can also use the resume or next command, which resumes the next connection in the user’s list of connections. This function allows you to create a single menu entry that steps through all of the user’s connections.

---

**Note**

A menu should not contain any exit paths that leave users in an unfamiliar interface environment.

When a particular line should always display a menu, that line can be configured with an autocommand line configuration command. Menus can be run on a per-user basis by defining a similar autocommand command for that local username. For more information about the autocommand command, see the Cisco IOS Dial Technologies Configuration Guide.

---

**Note**

The maximum number of menu commands that the device supports is 66.

---

**Examples**

In the following example, the commands to be issued when the menu user selects option 1, 2, or 3 are specified for the menu named Access1:

```
Device (config) #menu Access1 command 1 tn3270 vms.cisco.com
Device (config) #menu Access1 command 2 rlogin unix.cisco.com
Device (config) #menu Access1 command 3 menu-exit
```

The following example allows a menu user to exit a menu by entering Exit at the menu prompt:

```
menu Access1 text Exit Exit
menu Access1 command Exit menu-exit
```

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autocommand</td>
<td>Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.</td>
</tr>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td>menu clear-screen</td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an item.</td>
</tr>
<tr>
<td>menu options</td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
</tbody>
</table>
menu default

To specify the menu item to use as the default, use the menu default command in global configuration mode.

```
menu menu-name default menu-item
```

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu-name</td>
<td>Name of the menu. You can specify a maximum of 20 characters.</td>
</tr>
<tr>
<td>menu-item</td>
<td>Number, character, or string key of the item to use as the default.</td>
</tr>
</tbody>
</table>

Command Default

Disabled

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to specify which menu entry is used when the user presses Enter without specifying an item. The menu entries are defined by the menu command and menu text global configuration commands.

Examples

In the following example, the menu user exits the menu when pressing Enter without selecting an item:

```
menu Access1 9 text Exit the menu
menu Access1 9 command menu-exit
menu Access1 default
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a preconfigured user menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td>menu text</td>
<td>Specifies the text of a menu item in a user menu.</td>
</tr>
</tbody>
</table>
**menu line-mode**

To require the user to press Enter after specifying an item, use the `menu line-mode` command in global configuration mode.

```
menu  menu-name  line-mode
```

**Syntax Description**

- `menu-name` Name of the menu this command should be applied to.

**Command Default**

Enabled for menus with more than nine items. Disabled for menus with nine or fewer items.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In a menu of nine or fewer items, you ordinarily select a menu item by entering the item number. In line mode, you select a menu entry by entering the item number and pressing Enter. Line mode allows you to backspace over the selected number and enter another number before pressing Enter to issue the command.

This option is activated automatically when more than nine menu items are defined but also can be configured explicitly for menus of nine or fewer items.

In order to use strings as keys for items, the `menu line-mode` command must be configured.

**Examples**

In the following example, the line-mode option is enabled for the menu named Access1:

```
menu Access1 line-mode
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>menu (EXEC)</code></td>
<td>Invokes a preconfigured user menu.</td>
</tr>
<tr>
<td><code>menu clear-screen</code></td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td><code>menu command</code></td>
<td>Specifies underlying commands for a user menu.</td>
</tr>
<tr>
<td><code>menu default</code></td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td><code>menu options</code></td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td><code>menu prompt</code></td>
<td>Specifies the prompt for a user menu.</td>
</tr>
</tbody>
</table>
### menu options

To set options for items in user menus, use the **menu options** command in global configuration mode.

#### Syntax

```
Cisco IOS Release 10.0, 12.2(33)SRA, 12.2(33)SXI, and Later Releases
menu menu-name options menu-item [login] [pause]

Cisco IOS XE Release 3.1S and Later Releases
menu menu-name options menu-item {login|pause}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu-name</td>
<td>The name of the menu. You can specify a maximum of 20 characters.</td>
</tr>
<tr>
<td>menu-item</td>
<td>Number, character, or string key of the item affected by the option.</td>
</tr>
<tr>
<td>login</td>
<td>(Optional) Configures the router to request a login before issuing the command.</td>
</tr>
<tr>
<td>pause</td>
<td>(Optional) Configures the router to pause after issuing the command and before redrawing the menu.</td>
</tr>
</tbody>
</table>

#### Command Default

The menu options are disabled.

#### Command Modes

Global configuration (config)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 3.1S.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the **menu command** and **menu text** commands to define a menu entry.

#### Examples

The following example shows how to configure the router to request a login before issuing the command specified by menu entry 3 of the menu named Access1:

```
Router(config)#
menu Access1 options 3 login
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td>menu clear-screen</td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an item.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td>menu single-space</td>
<td>Displays menu items single-spaced rather than double-spaced.</td>
</tr>
<tr>
<td>menu status-line</td>
<td>Displays a line of status information about the current user at the top of a menu.</td>
</tr>
<tr>
<td>menu text</td>
<td>Specifies the text of a menu item in a user menu.</td>
</tr>
<tr>
<td>menu title</td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
</tbody>
</table>

**menu prompt**

To specify the prompt for a user menu, use the **menu prompt** command in global configuration mode.

```
menu menu-name prompt d prompt d
```

**Syntax Description**

<table>
<thead>
<tr>
<th>menu-name</th>
<th>Name of the menu. You can specify a maximum of 20 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote (&quot;), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.</td>
</tr>
<tr>
<td>prompt</td>
<td>Prompt string for the menu.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Press Enter after entering the first delimiter. The router will prompt you for the text of the prompt. Enter the text followed by the delimiter, and press Enter.

Use the **menu command** and **menu text** commands to define the menu selections.
Examples

In the following example, the prompt for the menu named Access1 is configured as “Select an item.”:

```
Router(config)# menu Access1 prompt /
Enter TEXT message. End with the character '/'.
Select an item. /
Router(config)#
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>menu</strong> (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td><strong>menu command</strong></td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td><strong>menu default</strong></td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td><strong>menu text</strong></td>
<td>Specifies the text of a menu item in a user menu.</td>
</tr>
<tr>
<td><strong>menu title</strong></td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
</tbody>
</table>

**menu status-line**

To display a line of status information about the current user at the top of a menu, use the `menu status-line` command in global configuration mode.

```
menu menu-name status-line
```

**Syntax Description**

- `menu-name`  
  Name of the menu this command should be applied to.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the status information at the top of the screen before the menu title is displayed. This status line includes the router’s host name, the user’s line number, and the current terminal type and keymap type (if any).

**Examples**

In the following example, status information is enabled for the menu named Access1:

```
menu Access1 status-line
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td>menu clear-screen</td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an item in a menu.</td>
</tr>
<tr>
<td>menu options</td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td>menu single-space</td>
<td>Displays menu items single-spaced rather than double-spaced.</td>
</tr>
<tr>
<td>menu text</td>
<td>Specifies the text of a menu item in a user menu.</td>
</tr>
<tr>
<td>menu title</td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
</tbody>
</table>

**menu text**

To specify the text of a menu item in a user menu, use the `menu text` command in global configuration mode.

```
menu menu-name text menu-item menu-text
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu-name</td>
<td>Name of the menu. You can specify a maximum of 20 characters.</td>
</tr>
<tr>
<td>menu-item</td>
<td>Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu items. When the tenth item is added to the menu, the <code>menu line-mode</code> and <code>menu single-space</code> commands are activated automatically.</td>
</tr>
<tr>
<td>menu-text</td>
<td>Text of the menu item.</td>
</tr>
</tbody>
</table>

**Command Default**

No text appears for the menu item.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to assign text to items in a menu. Use the `menu command` command to assign actions to items. These commands must use the same menu name and menu selection key.

You can specify a maximum of 18 items in a menu.
Examples

In the following example, the descriptive text for the three entries is specified for options 1, 2, and 3 in the menu named Access1:

```
menu Access1 text 1 IBM Information Systems
menu Access1 text 2 UNIX Internet Access
menu Access1 text 3 Exit menu system
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>menu (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td>menu clear-screen</td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td>menu command</td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td>menu default</td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td>menu line-mode</td>
<td>Requires the user to press Enter after specifying an item.</td>
</tr>
<tr>
<td>menu options</td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td>menu prompt</td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td>menu single-space</td>
<td>Displays menu items single-spaced rather than double-spaced.</td>
</tr>
<tr>
<td>menu status-line</td>
<td>Displays a line of status information about the current user at the top of a menu.</td>
</tr>
<tr>
<td>menu title</td>
<td>Creates a title, or banner, for a user menu.</td>
</tr>
</tbody>
</table>

**menu title**

To create a title (banner) for a user menu, use the **menu title** command in global configuration mode.

```
menu menu-name title d menu-title d
```

**Syntax Description**

<table>
<thead>
<tr>
<th>menu-name</th>
<th>Name of the menu. You can specify a maximum of 20 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>d</strong></td>
<td>A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash ((/)), double quote (&quot;&quot;), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.</td>
</tr>
<tr>
<td>menu-title</td>
<td>Lines of text to appear at the top of the menu.</td>
</tr>
</tbody>
</table>

**Command Default**

The menu does not have a title.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The `menu title` command must use the same menu name used with the `menu text` and `menu command` commands used to create a menu. You can position the title of the menu horizontally by preceding the title text with blank characters. You can also add lines of space above and below the title by pressing Enter. Follow the `title` keyword with one or more blank characters and a delimiting character of your choice. Then enter one or more lines of text, ending the title with the same delimiting character. You cannot use the delimiting character within the text of the message. When you are configuring from a terminal and are attempting to include special control characters, such as a screen-clearing string, you must use Ctrl-V before the special control characters so that they are accepted as part of the title string. The string `^[^[H^[J` is an escape string used by many VT100-compatible terminals to clear the screen. To use a special string, you must enter Ctrl-V before each escape character.

You also can use the `menu clear-screen` global configuration command to clear the screen before displaying menus and submenus, instead of embedding a terminal-specific string in the menu title. The `menu clear-screen` command allows the same menu to be used on different types of terminals.

In the following example, the title that will be displayed is specified when the menu named Access1 is invoked. Press Enter after the second slash (/) to display the prompt.

```
Router(config)# menu Access1 title `^[^[H^[J
Enter TEXT message. End with the character `/'.

Welcome to Access1 Internet Services

Type a number to select an option;
Type 9 to exit the menu.
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>menu</code> (EXEC)</td>
<td>Invokes a user menu.</td>
</tr>
<tr>
<td><code>menu clear-screen</code></td>
<td>Clears the terminal screen before displaying a menu.</td>
</tr>
<tr>
<td><code>menu command</code></td>
<td>Specifies underlying commands for user menus.</td>
</tr>
<tr>
<td><code>menu default</code></td>
<td>Specifies the menu item to use as the default.</td>
</tr>
<tr>
<td><code>menu line-mode</code></td>
<td>Requires the user to press Enter after specifying an item.</td>
</tr>
<tr>
<td><code>menu options</code></td>
<td>Sets options for items in user menus.</td>
</tr>
<tr>
<td><code>menu prompt</code></td>
<td>Specifies the prompt for a user menu.</td>
</tr>
<tr>
<td><code>menu single-space</code></td>
<td>Displays menu items single-spaced rather than double-spaced.</td>
</tr>
<tr>
<td><code>menu status-line</code></td>
<td>Displays a line of status information about the current user at the top of a menu.</td>
</tr>
</tbody>
</table>

Release | Modification
---|---
12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.
**microcode (12000)**

To load a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series Gigabit Switch Router (GSR), use the `microcode` command in global configuration mode. To load the microcode bundled with the GRP system image, use the `no` form of this command.

```
microcode {oc12-atm|oc12-pos|oc3-pos4} {flash file-id [slot]|system [slot]}
no microcode {oc12-atm|oc12-pos|oc3-pos4} [{flash file-id [slot]|system [slot]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oc12-atm</td>
<td>Interface name.</td>
</tr>
<tr>
<td>oc12-pos</td>
<td>Interface name.</td>
</tr>
<tr>
<td>oc3-pos4</td>
<td>Interface name.</td>
</tr>
<tr>
<td>flash</td>
<td>Loads the image from the Flash file system.</td>
</tr>
<tr>
<td>file-id</td>
<td>Specifies the device and filename of the image file to download from Flash memory. A colon (:) must separate the device and filename (for example, slot0:gsr-p-mz). Valid devices include:</td>
</tr>
<tr>
<td>system</td>
<td>Loads the image from the software image on the GRP card.</td>
</tr>
<tr>
<td>slot</td>
<td>Slot number of the line card that you want to copy the software image to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is downloaded on all line cards.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is to load the image from the GRP card (`system`).

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 GS</td>
<td>This command was introduced for Cisco 12000 series GSRs.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Normally, you want the same Cisco IOS image on the GRP card 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.

To load a Cisco IOS image on a line card, first use the `copy tftp` command to download the Cisco IOS image to a slot on one of the PCMCIA Flash memory cards. Then use the `microcode` command to download the image to the line card, followed by the `microcode reload` command to start the image. 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.

To verify that the correct image is running on the line card, use the `execute-on slot slot show version` command.

For additional information on GSR configuration, refer to the documentation specific to your Cisco IOS software release.

### Examples

In the following example, the Cisco IOS software image in slot 0 is downloaded to the line card in slot 10. This software image is used when the system is booted, a line card is inserted or removed, or the `microcode reload` global configuration command is issued.

```bash
Router(config)# microcode oc3-POS-4 flash slot0:fip.v141-7 10
Router(config)# microcode reload 10
```

In this example, the user would issue the `execute-on slot 10 show version` command to verify that the correct version is loaded.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>microcode reload (12000)</code></td>
<td>Reloads microcode on Cisco 12000 series GSRs.</td>
</tr>
</tbody>
</table>

### microcode (7000/7500)

To specify the location of the microcode that you want to download from Flash memory into the writable control store (WCS) on Cisco 7000 series (including RSP based routers) or Cisco 7500 series routers, use the `microcode` command in global configuration mode. To load the microcode bundled with the system image, use the `no` form of this command.

```bash
microcode interface-type {flash-filesystem:filename [slot] | rom | system [slot]}
no microcode interface-type {flash-filesystem:filename [slot] | rom | system [slot]}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-type</code></td>
<td>One of the following interface processor names: aip, cip, eip, feip, fip, fsip, hip, mip, sip, sp, ssp, trip, vip, or vip2</td>
</tr>
<tr>
<td><code>flash-filesystem</code></td>
<td>Flash file system, followed by a colon. Valid file systems are bootflash, slot0, and slot1</td>
</tr>
<tr>
<td></td>
<td>Slave devices such as slaveslot0 are invalid. The slave’s file system is not available during microcode reloads.</td>
</tr>
<tr>
<td><code>filename</code></td>
<td>Name of the microcode file.</td>
</tr>
<tr>
<td><code>slot</code></td>
<td>(Optional) Number of the slot. Range is from 0 to 15.</td>
</tr>
</tbody>
</table>
If the ROM is specified, the router loads from the onboard ROM microcode.

If the system keyword is specified, the router loads the microcode from the microcode bundled into the system image you are running for that interface type.

**Command Default**

The default is to load from the microcode bundled in the system image.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not use the `microcode reload` command after using the `microcode` command, the `microcode reload` command will be written to the configuration file automatically.

When using Dual RSPs for simple hardware backup, ensure that the master and slave RSP card contain the same microcode image in the same location when the router is to load the interface processor microcode from a Flash file system. Thus, if the slave RSP becomes the master, it will be able to find the microcode image and download it to the interface processor.

**Examples**

In the following example, all FIP cards will be loaded with the microcode found in Flash memory file `fip.v141-7` when the system is booted, when a card is inserted or removed, or when the `microcode reload` global configuration command is issued. The configuration is then written to the startup configuration file.

```
Router(config)# microcode fip slot0:fip.v141-7
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>more flh:logfile</code></td>
<td>Displays the system console output generated during the Flash load helper operation.</td>
</tr>
</tbody>
</table>

**microcode (7200)**

To configure a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router, use the `microcode` command in global configuration mode. To revert to the default microcode for the current running version of the Cisco IOS software, use the `no` form of this command.

```
microcode {ecpa|pcpa} location
no microcode {ecpa|pcpa}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eapa</td>
<td>ESCON Channel Port Adapter (CPA) interface.</td>
</tr>
<tr>
<td>pcpa</td>
<td>Parallel CPA interface.</td>
</tr>
</tbody>
</table>
**Command Default**

If the default or no form of the command is specified, the driver uses the default microcode for the current running version of the Cisco IOS software.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If there are any default overrides when the configuration is written, then the `microcode reload` command will be written to the configuration automatically. This action enables the configured microcode to be downloaded at system startup.

The CPA microcode image is preloaded on Flash memory cards for Cisco 7200-series routers for Cisco IOS Release 11.3(3)T and later releases. You may be required to copy a new image to Flash memory when a new microcode image becomes available.

For more information on the CPA configuration and maintenance, refer to the “Configuring Cisco Mainframe Channel Connection Adapters” chapter in the *Release 12.2 Cisco IOS Bridging and IBM Networking Configuration Guide.*

**Examples**

The following example instructs the Cisco IOS software to load the microcode from an individual microcode image that is stored as a file on the Flash card inserted in Flash card slot 0:

```
microcode ecpa slot0:xcpa26-1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>microcode reload</code></td>
<td>Resets and reloads the specified hardware in a Cisco 7200 series router.</td>
</tr>
<tr>
<td><code>show microcode</code></td>
<td>Displays microcode information.</td>
</tr>
</tbody>
</table>

**microcode reload (12000)**

To reload the Cisco IOS image from a line card on Cisco 12000 series routers, use the `microcode reload` command in global configuration mode.

```
microcode reload [slot-number]
```

**Syntax Description**

| slot-number | (Optional) Slot number of the line card that you want to reload the Cisco IOS software image on. Slot numbers range from 0 to 11 for the Cisco 12012 and from 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is reloaded on all line cards. |
**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 GS</td>
<td>This command was introduced for Cisco 12000 series GSRs.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Normally, you want the same Cisco IOS image on the GRP card 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 different Cisco IOS image. Additionally, you might need to load a new image on the line card to work around a problem affecting only one of the line cards.

To load a Cisco IOS image on a line card, first use the `copy tftp` command to download the Cisco IOS image to a slot on one of the PCMCIA Flash memory cards. Then use the `microcode` command to download the image to the line card, followed by the `microcode reload` command to start the image. To verify that the correct image is running on the line card, use the `execute-on slot slot show version` command.

For additional information on GSR configuration, refer to the “Observing System Startup and Performing a Basic Configuration” chapter in the Cisco 12000 series installation and configuration guides.

The `microcode reload` (12000) command allows you to issue another command immediately.

**Note**

Issuing a `microcode reload` command on any of the line cards in a Cisco 12000 GSR immediately returns the console command prompt. This allows you to issue a subsequent command immediately to the reloading line card. However, any commands entered at this time will not execute, and often no indication will be given that such a command failed to run. Verify that the microcode has reloaded before issuing new commands.

**Examples**

In the following example, the mirocode firmware is reloaded on the line card in slot 10:

```
Router(config)# microcode reload 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>microcode</td>
<td>Loads a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series GSR.</td>
</tr>
<tr>
<td>(12000)</td>
<td></td>
</tr>
</tbody>
</table>

**microcode reload (7000 7500)**

To reload the processor card on the Cisco 7000 series with RSP7000 or Cisco 7500 series routers, use the `microcode reload` command in global configuration mode.

```
microcode reload [slot-number]
```
Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot-number</td>
<td>(Optional) Reloads the specified processor card slot on a Cisco 7500 series router.</td>
</tr>
</tbody>
</table>

Command Default

No default behaviors or values.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced for Cisco 7500 series routers.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The slot-number argument was added for Cisco 7500 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command reloads the microcode without rebooting the router. Immediately after you enter the microcode reload command, the system reloads all microcode. Global configuration mode remains enabled.

Note

If you modify the system configuration to load a microcode image, the microcode reload command will be written to the configuration file automatically following the use of a microcode command. This action enables the configured microcode to be downloaded at system startup.

Examples

In the following example, all controllers are reset, and the microcode specified in the current configuration is loaded:

Router(config)# microcode reload

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>microcode (7000/7500)</td>
<td>Specifies the location from where microcode should be loaded when the microcode reload command is processed on RSP-based routers.</td>
</tr>
</tbody>
</table>

microcode reload (7200)

To reload the Cisco IOS microcode image on an ESCON CPA card in the Cisco 7200 series router, use the microcode reload command in privileged EXEC mode.

microcode reload {all|ecpa [slot slot-number]|pcpa [slot slot-number]}

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Resets and reloads all hardware types that support downloadable microcode.</td>
</tr>
<tr>
<td>ecpa</td>
<td>Resets and reloads only those slots that contain hardware type ecpa.</td>
</tr>
<tr>
<td>pcpa</td>
<td>Resets and reloads only those slots that contain hardware type pcpa.</td>
</tr>
<tr>
<td>slot slot-number</td>
<td>(Optional) Resets and reloads only the slot specified, and only if it contains the hardware specified.</td>
</tr>
</tbody>
</table>
mkdir

To create a new directory in a Class C flash file system, use the `mkdir` command in user EXEC, privileged EXEC, or diagnostic mode.

```
mkdir directory
```

**Syntax Description**

- `directory` The name of the directory to create.

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
This command was modified and implemented on the Cisco ASR 1000 Aggregation Services Routers. The following enhancements were made:

- This command was introduced in diagnostic mode. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers.
- The harddisk:, obfl:, stby-harddisk:, stby-nvram:, stby-obfl:, stby-usb[0-1];, and usb[0-1]: directory options were added.

Usage Guidelines

This command is valid only on Class C flash file systems.

When executing the `mkdir directory` command on a USB token device, you can create only two levels of subdirectories under a directory. A new directory (third level directory) cannot be created on the USB token, but you can copy files to the existing subdirectories.

Examples

The following example creates a directory named newdir:

```plaintext
Router# mkdir newdir
Mkdir file name [newdir]? 
Created dir flash:newdir
```

```plaintext
Router# dir
Directory of flash:
  drwx   0 Mar 13 1993 13:16:21 newdir
8128000 bytes total (8126976 bytes free)
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dir</code></td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td><code>rmdir</code></td>
<td>Removes an existing directory in a Class C flash file system.</td>
</tr>
</tbody>
</table>

`mkdir disk0:`

To create a new directory in a Flash file system, use the `mkdir disk0:` command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command has no default settings.

**Command Modes**

EXEC

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
<td></td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.</td>
<td></td>
</tr>
</tbody>
</table>
### mkdir

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

#### Usage Guidelines

This command is valid only on Flash file systems.

After you enter the `mkdir disk0:` command, you are prompted to enter the new directory filename.

To check your entry, enter the `dir` command.

To remove a directory, enter the `rmdir` command.

#### Examples

This example shows how to create a directory named newdir:

```
Router# mkdir disk0:
Create directory filename [ ]? newdir
Created dir disk0: newdir
Router#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cd</code></td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td><code>dir</code></td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td><code>rmdir</code></td>
<td>Removes an existing directory in a Class C Flash file system.</td>
</tr>
</tbody>
</table>

### mode

To set the redundancy mode, use the `mode` command in redundancy configuration mode.

#### Syntax for 12.2S Release

`mode {rpr|rpr-plus|sso}`

#### Syntax for Cisco IOS XE Release 2.5 and Later Releases

`mode {rpr|sso}`

#### Syntax for 12.2XNE Release

`mode sso`

#### Syntax Description

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rpr</code></td>
<td>Specifies Route Processor Redundancy (RPR) mode.</td>
</tr>
<tr>
<td><code>rpr-plus</code></td>
<td>Specifies Route Processor Redundancy Plus (RPR+) mode.</td>
</tr>
<tr>
<td><code>sso</code></td>
<td>Specifies stateful switchover (SSO) mode.</td>
</tr>
</tbody>
</table>

#### Command Default

- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.
If redundancy is enabled, the default is the mode that you have configured.

The default is RPR+ mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.

The default is RPR mode if different versions are installed.

If redundancy is enabled, the default is the mode that you have configured.

The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.

The default is RPR mode if different versions are installed.

The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.

The default is RPR mode if different versions are installed.

Command Modes

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17b)SX</td>
<td>This command was modified. Support was added for SSO mode and the default mode change.</td>
</tr>
<tr>
<td>12.2(17d)SX</td>
<td>This command was modified. Support was added for multicast and unicast traffic.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)XNE</td>
<td>This command was modified. This command was implemented on the Cisco 10000 router.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was modified. This command was implemented on the Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Cisco IOS Release 12.2S and 7600 Series Routers

SSO is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

On releases prior to Release 12.2(17d)SX, single router mode (SRM) with SSO redundancy does not support stateful switchover for multicast traffic. When a switchover occurs, all multicast hardware switching entries are removed and are then re-created and reinstalled in the hardware by the newly active multilayer switch feature card (MSFC).

SRM/SSO is supported in the following releases only:

- Release 12.2(17b)SX and subsequent rebuilds.
- Release 12.2(17d)SX and subsequent rebuilds.

Nonstop forwarding (NSF) with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).
If you have configured MPLS on the Cisco 7600 series routers with redundant supervisor engines, you must configure the Cisco 7600 series router in RPR mode. The switch should not be running in the default mode of SSO.

Enter the `redundancy` command in global configuration mode to enter redundancy configuration mode. You can enter the `mode` command within redundancy configuration mode.

Follow these guidelines when configuring your system for RPR+ mode:

- You must install compatible images on the active and standby supervisor engines to support RPR+ mode and SSO mode.
- Both supervisor engines must run the same Cisco IOS software version.
- Any modules that are not online at the time of a switchover are reset and reloaded on a switchover.
- The Forwarding Information Base (FIB) tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.

The standby supervisor engine reloads on any change of mode and begins to work in the current mode. When you use this command to force the standby supervisor engine to run as a Distributed Forwarding Card (DFC) card, the uplink ports in the standby engine continue to be in use and are not disabled.

**Cisco IOS Release XE Release 2.5 and ASR 1000 Series Routers**

For Cisco ASR 1002 and 1004 routers, RRP and stateful switchover can be used to switch between Cisco IOS processes. RPR and SSO need to be configured by the user, however, because a second Cisco IOS process is not available by default on Cisco ASR 1002 and 1004 routers. Enter the `redundancy` command in global configuration mode to enter redundancy configuration mode. You can enter the `mode` command within redundancy configuration mode.

The Cisco ASR 1006 Router supports a second Route Processor. The second Cisco IOS process can run only on the standby Route Processor. This means that hardware redundancy is available and RPR and SSO do not need to be configured by the user because a second Cisco IOS process is available by default on the Cisco ASR 1006 router.

RPR+ mode is not supported on the Cisco ASR 1000 Series Routers.

**Cisco IOS Release 12.2XNE and 1000 Series Routers**

Enter the `redundancy` command in global configuration mode to enter redundancy configuration mode. You can enter the `mode` command within redundancy configuration mode.

RPR mode is not supported on the Cisco 10000 router.

**Examples**

This example shows how to set the redundancy mode to RPR+:

```
Router(config)# redundancy
Router(config-red)# mode rpr-plus
```

This example shows how to set the redundancy mode to SSO:

```
Router(config)# redundancy
Router(config-red)# mode sso
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy</td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td>redundancy force-switchover</td>
<td>Forces a switchover from the active to the standby supervisor engine.</td>
</tr>
<tr>
<td>route-converge-interval</td>
<td>Configures the time interval after which the old FIB entries are purged.</td>
</tr>
<tr>
<td>show redundancy</td>
<td>Displays RF information.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>
Through mode
monitor event-trace through Q

- monitor event-trace through Q, on page 318
monitor event-trace through Q

monitor event-trace (EXEC)

To monitor and control the event trace function for a specified Cisco IOS software subsystem component, use the `monitor event-trace` command in privileged EXEC mode.

```
monitor event-trace component {clear|continuous|destroy-buffer|disable|dump [pretty]|enable|one-shot}
```

Cisco 10000 Series Routers
```
monitor event-trace component {disable|dump|enable|size|stacktrace}
```

Catalyst 6500 Series Switches and Cisco 7600 Series Routers
```
monitor event-trace all-traces {continuous [cancel]|dump [merged] [pretty]}
monitor event-trace l3 {clear|continuous [cancel]|disable|dump [pretty]|enable|interface type mod/port|one-shot}
monitor event-trace spa {clear|continuous [cancel]|disable|dump [pretty]|enable|one-shot}
monitor event-trace subsys {clear|continuous [cancel]|disable|dump [pretty]|enable|one-shot}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>component</code></td>
<td>Name of the Cisco IOS software subsystem component that is the subject of the event trace. To get a list of components that support event tracing, use the <code>monitor event-trace ?</code> command.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears existing trace messages for the specified component from memory on the networking device.</td>
</tr>
<tr>
<td>continuous</td>
<td>Continuously displays the latest event trace entries.</td>
</tr>
<tr>
<td>destroy-buffer</td>
<td>Clears the buffer (in volatile memory) of the trace data. Relevant only for subscriber ppp event.</td>
</tr>
<tr>
<td>disable</td>
<td>Turns off event tracing for the specified component.</td>
</tr>
<tr>
<td>dump</td>
<td>Writes the event trace results to the file configured using the <code>monitor event-trace</code> command in global configuration mode. The trace messages are saved in binary format.</td>
</tr>
<tr>
<td>pretty</td>
<td>(Optional) Saves the event trace message in ASCII format.</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on event tracing for the specified component.</td>
</tr>
<tr>
<td>one-shot</td>
<td>Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the <code>monitor event-trace</code> command in global configuration mode.</td>
</tr>
</tbody>
</table>
Set the number of messages that can be written to memory for a single instance of a trace.

**Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the `show monitor event-trace component parameters` command.

When the number of event trace messages in memory exceeds the size, new messages will begin to overwrite the older messages in the file.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes Privileged EXEC (#)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(18)S</td>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(8)T.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td></td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S. The <code>monitor event-trace cef ipv4 clear</code> command replaces the <code>clear ip cef event-log</code> command.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>IOS XE Fuji 16.9.1</td>
<td></td>
<td>The subscriber ppp component was added, and the <code>destroy-buffer</code> keyword was added for use with this component.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use the `monitor event-trace` command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the `monitor event-trace` command in global configuration mode.

The amount of data collected from the trace depends on the trace message size configured using the `monitor event-trace` command in global configuration mode for each instance of a trace.

Note

The Cisco IOS software allows for the subsystem components to define whether support for event tracing is enabled or disabled at boot time. You can enable or disable event tracing in two ways: using the `monitor event-trace` command in privileged EXEC mode or using the `monitor event-trace` command in global configuration mode. To disable event tracing, you would enter either of these commands with the `disable` keyword. To enable event tracing again, you would enter either of these commands with the `enable` keyword.

To determine whether you can enable event tracing on a subsystem, use the `monitor event-trace ?` command to get a list of software components that support event tracing. To determine whether event tracing is enabled by default for the subsystem, use the `show monitor event-trace` command to display trace messages.

Use the `show monitor event-trace` command to display trace messages. Use the `monitor event-trace component dump` command to save trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the `monitor event-trace component dump pretty` command.

To write the trace messages for all events currently enabled on a networking device to a file, enter the `monitor event-trace dump` command.

To configure the file where you want to save trace information, use the `monitor event-trace` command in global configuration mode. The trace messages are saved in a binary format.

Examples

The following example shows the privileged EXEC commands to stop event tracing, clear the current contents of memory, and reenable the trace function for the interprocess communication (IPC) component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace ipc disable
Router# monitor event-trace ipc clear
Router# monitor event-trace ipc enable
```

The following example shows how the `monitor event-trace one-shot` command accomplishes the same function as the previous example except in one command. In this example, once the size of the trace message file has been exceeded, the trace is terminated.

```
Router# monitor event-trace ipc one-shot
```

The following example shows the command for writing trace messages for an event in binary format. In this example, the trace messages for the IPC component are written to a file.

```
Router# monitor event-trace ipc dump
```

The following example shows the command for writing trace messages for an event in ASCII format. In this example, the trace messages for the MBUS component are written to a file.
Router# monitor event-trace mbus dump pretty

Catalyst 6500 Series Switches and Cisco 7600 Series Routers Examples Only

This example shows how to stop event tracing, clear the current contents of memory, and reenable the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>monitor event-trace (global)</td>
<td>Configures event tracing for a specified Cisco IOS software subsystem component.</td>
</tr>
<tr>
<td></td>
<td>monitor event-trace dump-traces</td>
<td>Saves trace messages for all event traces currently enabled on the networking device.</td>
</tr>
<tr>
<td></td>
<td>show monitor event-trace</td>
<td>Displays event trace messages for Cisco IOS software subsystem components.</td>
</tr>
</tbody>
</table>

**monitor event-trace (global)**

To configure event tracing for a specified Cisco IOS software subsystem component, use the `monitor event-trace` command in global configuration mode.

```plaintext
monitor event-trace component {disable|dump-file filename|enable|size number|stacktrace number} timestamps [{datetime | localtime | msec | show-timezone | uptime}]
```

Cisco 10000 Series Routers

```plaintext
monitor event-trace component {disable|dump-file filename|enable|clear|continuous|one-shot}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>component</th>
<th>Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing, use the <code>monitor event-trace ?</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>disable</td>
<td>Turns off event tracing for the specified component.</td>
</tr>
<tr>
<td></td>
<td>dump-file filename</td>
<td>Specifies the file where event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Turns on event tracing for the specified component provided that the component has been configured using the <code>monitor event-trace</code> command.</td>
<td></td>
</tr>
</tbody>
</table>
| **size number** | Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from 1 to 65536.  
**Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the `show monitor event-trace component/parameters` command.  
When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file. |
| **stacktrace number** | Enables the stack trace at tracepoints and specifies the depth of the stack trace stored. Valid values are from 1 to 16. |
| **timestamps** | (Optional) Includes time stamp information with the event trace messages for the specified component. |
| **datetime** | (Optional) Specifies that the time stamp information included with event trace messages will consist of the date and time of the event trace. |
| **localtime** | (Optional) Specifies that the time given in the time stamp will be local time. |
| **msec** | (Optional) Includes milliseconds in the time stamp. |
| **show-timezone** | (Optional) Includes time zone information in the time stamp. |
| **uptime** | (Optional) Displays time stamped information about the system uptime. |
| **clear** | Clears existing trace messages for the specified component from memory on the networking device. |
| **continuous** | Continuously displays the latest event trace entries. |
| **one-shot** | Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the `monitor event-trace` command. |

**Command Default**

Event tracing is enabled or disabled depending on the software component.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(18)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(8)T.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>
Modification Release

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `monitor event-trace` command to enable or disable event tracing and to configure event trace parameters for Cisco IOS software subsystem components.

**Note**

Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative. In Cisco IOS software images that do not provide subsystem support for the event trace function, the `monitor event-trace` command is not available.

The Cisco IOS software allows the subsystem components to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default two ways: using the `monitor event-trace` command in privileged EXEC mode or using the `monitor event-trace` command in global configuration mode.

Additionally, default settings do not show up in the configuration file. If the subsystem software enables event tracing by default, the `monitor event-trace component enable` command will not show up in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.

**Note**

The amount of data collected from the trace depends on the trace message size configured using the `monitor event-trace` command for each instance of a trace.

To determine whether you can enable event tracing on a subsystem, use the `monitor event-trace ?` command to get a list of software components that support event tracing.

To determine whether event tracing is enabled by default for the subsystem, use the `show monitor event-trace` command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

**Examples**

The following example shows how to enable event tracing for the interprocess communication (IPC) subsystem component in Cisco IOS software and configure the size to 4096 messages. The trace messages file is set to `ipc-dump` in slot0 (flash memory).

```
configure terminal
!
monitor event-trace ipc enable
monitor event-trace ipc dump-file slot0:ipc-dump
monitor event-trace ipc size 4096
```

When you select Cisco Express Forwarding as the component for which to enable event tracing, you can use the following additional arguments and keywords: `monitor event-trace cef [events] [interface`
The following examples show how to enable event tracing for IPv4 or IPv6 events of the Cisco Express Forwarding component in Cisco IOS software:

```
configure terminal
! monitor event-trace cef ipv4 enable
configure terminal
! monitor event-trace cef ipv6 enable
exit
```

The following example shows what happens when you try to enable event tracing for a component (in this case, adjacency events) when it is already enabled:

```
configure terminal
! monitor event-trace adjacency enable
%EVENT_TRACE-6-ENABLE: Trace already enabled.
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>monitor event-trace (EXEC)</strong></td>
<td>Controls the event trace function for a specified Cisco IOS software subsystem component.</td>
</tr>
<tr>
<td><strong>monitor event-trace dump-traces</strong></td>
<td>Saves trace messages for all event traces currently enabled on the networking device.</td>
</tr>
<tr>
<td><strong>show monitor event-trace</strong></td>
<td>Displays event trace messages for Cisco IOS software subsystem components.</td>
</tr>
</tbody>
</table>

### monitor event-trace dump-traces

To save trace messages for all event traces currently enabled on the networking device, use the `monitor event-trace dump-traces` command in privileged EXEC mode.

```
monitor event-trace dump-traces [pretty]
```

#### Syntax Description

| pretty | (Optional) Saves the event trace message in ASCII format. |

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(18)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(8)T.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the `monitor event-trace dump-traces` command to save trace message information for all event traces currently enabled on a networking device. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the `monitor event-trace dump-traces pretty` command.
To write the trace messages for an individual trace event to a file, enter the `monitor event-trace` (EXEC) command.

To configure the file where you want to save messages, use the `monitor event-trace` (global) command.

**Examples**

The following example shows how to save the trace messages in binary format for all event traces enabled on the networking device.

```
monitor event-trace dump-traces
```

The following example shows how to save the trace messages in ASCII format for all event traces enabled on the networking device.

```
monitor event-trace dump-traces pretty
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor event-trace</code></td>
<td>Controls event trace function for a specified Cisco IOS software subsystem component.</td>
</tr>
<tr>
<td>(EXEC)</td>
<td></td>
</tr>
<tr>
<td><code>monitor event-trace</code></td>
<td>Configures event tracing for a specified Cisco IOS software subsystem component.</td>
</tr>
<tr>
<td>(global)</td>
<td></td>
</tr>
<tr>
<td><code>show monitor event-trace</code></td>
<td>Displays event trace messages for Cisco IOS software subsystem components.</td>
</tr>
</tbody>
</table>

**monitor pcm-tracer capture-destination**

To configure a location to save the Pulse Code Modulation (PCM) trace information, use the `monitor pcm-tracer capture-destination` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
monitor pcm-tracer capture-destination destination
no monitor pcm-tracer capture-destination
```
**Syntax Description**

<table>
<thead>
<tr>
<th>destination</th>
<th>Destination to save the PCM trace information. You can specify any of the following values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>--Saves trace to archive.</td>
</tr>
<tr>
<td>flash</td>
<td>--Saves trace to flash memory.</td>
</tr>
<tr>
<td>ftp</td>
<td>--Saves trace to an FTP network server.</td>
</tr>
<tr>
<td>http</td>
<td>--Saves trace to an HTTP server.</td>
</tr>
<tr>
<td>https</td>
<td>--Saves trace to a secure HTTP (HTTPS) server.</td>
</tr>
<tr>
<td>null</td>
<td>--Saves trace to file system.</td>
</tr>
<tr>
<td>nvram</td>
<td>--Saves trace to the NVRAM of the router.</td>
</tr>
<tr>
<td>pram</td>
<td>--Saves trace to the permanent RAM (PRAM) of the router.</td>
</tr>
<tr>
<td>rcp</td>
<td>--Saves trace to a remote copy protocol (RCP) network server.</td>
</tr>
<tr>
<td>scp</td>
<td>--Saves trace to a network server that supports Secure Shell (SSH).</td>
</tr>
<tr>
<td>syslog</td>
<td>--Saves trace to the system log.</td>
</tr>
<tr>
<td>system</td>
<td>--Saves trace to the system memory.</td>
</tr>
<tr>
<td>tftp</td>
<td>--Saves trace to a TFTP network server.</td>
</tr>
<tr>
<td>tmpsys</td>
<td>--Saves trace to a temporary system location.</td>
</tr>
</tbody>
</table>

**Command Default**

The PCM trace information is saved to the NVRAM.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the `monitor pcm-tracer capture-destination` command to specify a location to save the PCM trace information. When Cisco IOS software saves the data to network file systems, such as TFTP and FTP, it assumes the location is valid and has write access.

After the PCM capture is complete, the router automatically copies the captured contents to the specified location. The filename format at the destination location is as follows:

```
<Configured name>_tx_<DS0 slot>_x_DS0 unit>_x_DS0 channel>--For TX
<Configured name>_rx_<DS0 slot>_x_DS0 unit>_x_DS0 channel>--For RX
```

You can identify the dial feature card (DFC) channel from where the PCM is traced using the filename format.

Consider the following example:

Router(config)# monitor pcm-tracer capture-destination tftp://223.255.254.254/benzeer/cap/cap_data
In this example, two files are created for the data corresponding to each DS0s, one for each direction (transmitter and receiver). When the `debug pcmtracer` command is enabled, the trace data is copied into the following files:

- `cap_data_tx_6_1_22` and `cap_data_rx_6_1_22`--This corresponds to the traffic flowing through DS0 6/1:22.
- `cap_data_tx_6_1_22` and `cap_data_rx_6_1_22`--`cap_data_tx_6_1_22` is the data in the transmit direction (from the DFC to the system backplane) and `cap_data_rx_6_1_22` is the data in the receiver direction (to the DFC from the system backplane).

### Examples

The following example shows how to configure a router to save the PCM trace information to a flash drive:

```bash
Router# configure terminal
Router(config)# monitor pcm-tracer capture-destination flash:
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug pcmtracer</code></td>
<td>Enables debugging for PCM tracing.</td>
</tr>
<tr>
<td><code>monitor pcm-tracer</code></td>
<td>Monitors and controls the PCM trace function.</td>
</tr>
</tbody>
</table>

### monitor pcm-tracer delayed-start

To configure the delay time to start the Pulse Code Modulation (PCM) trace capture, use the `monitor pcm-tracer delayed-start` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```bash
monitor pcm-tracer delayed-start seconds
no monitor pcm-tracer delayed-start
```

**Syntax Description**

| `seconds` | Delay, in seconds. The range is from 1 to 2147483. |

**Command Default**

The default delay time is zero.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the PCM tracer delay time to 1000 seconds:

```bash
Router# configure terminal
Router(config)# monitor pcm-tracer delayed-start 1000
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor pcm-tracer</td>
<td>Configures the PCM tracer information.</td>
</tr>
</tbody>
</table>

**monitor pcm-tracer profile**

To create Pulse Code Modulation (PCM) capture profiles, use the **monitor pcm-tracer profile** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
monitor pcm-tracer profile profile-number
  { [no] capture-tdm [{[T1|E1]}]|[analog-voice-port|bri-voice-port]port|ds0|channel-num number} }
no monitor pcm-tracer profile profile-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile-number</td>
<td>Profile number. The range is from 1 to 10.</td>
</tr>
<tr>
<td>capture-tdm</td>
<td>(Optional) Set up ds0 dumps on specified ports</td>
</tr>
<tr>
<td>T1</td>
<td>(Optional) Specifies a ds0 dump on a T1 voice port.</td>
</tr>
<tr>
<td>E1</td>
<td>(Optional) Specifies a ds0 dump on an E1 voice port.</td>
</tr>
<tr>
<td>analog-voice-port</td>
<td>(Optional) Specifies a ds0 dump on an analog voice port.</td>
</tr>
<tr>
<td>bri-voice-port</td>
<td>(Optional) Specifies a ds0 dump on a BRI voice port.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) The specific port name.</td>
</tr>
<tr>
<td>ds0</td>
<td>(Optional) Specifies a ds0 dump.</td>
</tr>
<tr>
<td>channel-num</td>
<td>(Optional) Specifies a channel number for the dump.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Specific number of the channel.</td>
</tr>
</tbody>
</table>

**Command Default**

PCM capture profiles are disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must create at least one user profile under the channels that need to be traced. You can create the following profile operations:

- Create a user profile identified by a profile number.
- Add one or more profiles. A user profile consists of capture groups in which the channels that are to be traced are specified.
- Configure one or more capture groups under a profile.
Examples

The following example shows how to create a PCM capture profile with profile number 1:

```
Router# configure terminal
Router(config)# monitor pcm-tracer profile 1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor pcm-tracer</td>
<td>Configures the PCM tracer information.</td>
</tr>
</tbody>
</table>

### monitor permit-list

To configure a destination port permit list or add to an existing destination port permit list, use the `monitor permit-list` command in global configuration mode. To delete from or clear an existing destination port permit list, use the `no` form of this command.

**Activate monitoring**

```
monitor permit-list
no monitor permit-list
```

**Activate monitoring on one port**

```
monitor permit-list destination interface interface-type slot/port
no monitor permit-list destination interface interface-type slot/port
```

**Activate monitoring on one range of ports**

```
monitor permit-list destination interface interface-type slot/port-last-port
no monitor permit-list destination interface interface-type slot/port-last-port
```

**Activate monitoring on two or more ranges of ports**

```
monitor permit-list destination interface interface-type slot/port-last-port, [port-last-port]
no monitor permit-list destination interface interface-type slot/port-last-port, [port-last-port]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>destination</th>
<th>Specifies a destination port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specifies the interface type; valid values are <code>ethernet</code>, <code>fastethernet</code>, <code>gigabitethernet</code>, or <code>tengigabitethernet</code></td>
</tr>
<tr>
<td>slot</td>
<td>The slot that the interface module is installed in.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a single port on an interface module, or the first port on an interface module used in a range of ports.</td>
</tr>
<tr>
<td>last-port</td>
<td>(Optional) Specifies the port on an interface module used as the last port in a range of ports.</td>
</tr>
<tr>
<td>,</td>
<td>(Optional) Separates each instance of a port, or range of ports, that are monitored. See the Usage Guidelines and the Examples for more information.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled
Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXE</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To prevent accidental configuration of ports as destinations, you can create a permit list of the ports that are valid for use as destinations. With a destination port permit list configured, you can only configure the ports in the permit list as destinations.

When you enter multiple instances of `interface interface-type slot/port-fastport`, you must enter a space before and after the comma. For example, `interface interface-type slot/port-fastport , interface-type slot/port-fastport , interface-type slot/port-fastport`.

Examples

This example shows how to configure a destination port permit list that includes Gigabit Ethernet ports 5/1 through 5/4, and activate monitoring:

```
Router# configure terminal
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4
Router(config)#
```

This example shows how to configure a destination port permit list that includes Fast Ethernet ports 1/1-48, 2/1-48, and Gigabit Ethernet ports 3/1 through 3/4, and activate monitoring:

```
Router# configure terminal
Router(config)# monitor permit-list destination interface fastEthernet 1/1-48 , fastEthernet 2/1-48 , gigabitEthernet 3/1-4
Router(config)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show monitor permit-list</code></td>
<td>Displays the permit-list state and interfaces configured.</td>
</tr>
</tbody>
</table>

monitor session egress replication-mode

To switch the egress-span mode from the default mode (either centralized or distributed depending on your Cisco IOS software release), use the `monitor session egress replication-mode` command in global configuration mode. To return to the default mode, use the `no` form of the command.

**Cisco IOS Release 12.2(33)SXH2a and Later Releases**

- `monitor session egress replication-mode centralized`
- `no monitor session egress replication-mode centralized`

**Cisco IOS Release 12.2(33)SXH, SXH1, and SXH2**

- `monitor session egress replication-mode distributed`
- `no monitor session egress replication-mode distributed`
Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>centralized</td>
<td>In Cisco IOS Release 12.2(33)SXH2a and later releases: Specifies centralized egress span monitoring as the default mode.</td>
</tr>
<tr>
<td>distributed</td>
<td>In Cisco IOS Release 12.2(33)SXH, SXH1, and SXH2: Specifies distributed egress span monitoring as the default mode.</td>
</tr>
</tbody>
</table>

Command Default

Cisco IOS Releases 12.2(33)SXH2a and later releases: Centralized mode
Cisco IOS Releases 12.2(33)SXH, SXH1, and SXH2: Distributed mode

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXH2a</td>
<td>The command was changed as follows:</td>
</tr>
<tr>
<td></td>
<td>• The default mode was changed from distributed mode to centralized mode.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>centralized</strong> keyword was removed and the <strong>distributed</strong> keyword was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

**Note**

Prior to Cisco IOS Release 12.2(33)SXH and the introduction of this feature, the operating mode was centralized and could not be changed.

Centralized egress span monitoring redirects traffic to the supervisor engine for egress monitoring.

Distributed egress span monitoring is performed in the ingress module. Distributed replication for Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), and Encapsulated RSPAN (ERSPAN) increases the total throughput at the span destination.

**Note**

Distributed egress span (DES) mode is applied to ASIC-based sessions only.

Examples

**Cisco IOS Release 12.2(33)SXH, SXH1, and SXH2**

The following example shows how to switch the egress-span mode from the distributed default to centralized mode:

```
Router(config)# monitor session egress replication-mode centralized
```

The following example shows how to switch the egress-span mode from centralized back to distributed mode:

```
Router(config)# no monitor session egress replication-mode centralized
```
Cisco IOS Release 12.2(33)SXH2a and Later Releases

The following example shows how to switch the egress-span mode from the centralized default to distributed mode:

Router(config)# monitor session egress replication-mode distributed

The following example shows how to switch the egress-span mode from distributed back to centralized mode:

Router(config)# no monitor session egress replication-mode distributed

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor session</td>
<td>Displays the operational mode and configured mode of the session and module session capabilities.</td>
</tr>
</tbody>
</table>

monitor session type

To configure a local Switched Port Analyzer (SPAN), RSPAN, or ERSPAN, use the `monitor session type` command in global configuration mode. To remove one or more source or destination interfaces from the SPAN session, use the `no` form of this command.

```
monitor session span-session-number type {erspan-destination|erspan-source|local|local-tx|rspan-destination|rspan-source}
no monitor session span-session-number type {erspan-destination|erspan-source|local|local-tx|rspan-destination|rspan-source}
```

Syntax Description

<table>
<thead>
<tr>
<th>span-session-number</th>
<th>Number of the local SPAN or ERSPAN session; valid values are from 1 to 66.</th>
</tr>
</thead>
<tbody>
<tr>
<td>erspan-destination</td>
<td>Specifies the ERSPAN destination-session configuration mode.</td>
</tr>
<tr>
<td>erspan-source</td>
<td>Specifies the ERSPAN source-session configuration mode.</td>
</tr>
<tr>
<td>local</td>
<td>Specifies the local SPAN session configuration mode.</td>
</tr>
<tr>
<td>local-tx</td>
<td>Specifies the local egress-only SPAN session configuration mode.</td>
</tr>
<tr>
<td>rspan-destination</td>
<td>Specifies the RSPAN destination-session configuration mode.</td>
</tr>
<tr>
<td>rspan-source</td>
<td>Specifies the RSPAN source-session configuration mode.</td>
</tr>
</tbody>
</table>

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>
Modification

Release 12.2(18)SXF
This command was changed as follows:
- Support for this command was introduced on the Supervisor Engine 32.
- ERSPAN is supported in any switch fabric module functionality switching mode.

Release 12.2(33)SXH
This command was changed to include the following keywords:
- local
- local-tx
- rspan-destination
- rspan-source

Usage Guidelines

Release 12.2(18)SXE and later releases support ERSPAN with the Supervisor Engine 720, hardware revision 3.2 or higher. Enter the show module version | include WS-SUP720-BASE command to display the hardware revision.

ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

This command is not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

All ERSPAN source sessions on a switch must use the same source IP address. You enter the origin ip address command to configure the IP address for the ERSPAN source sessions.

All ERSPAN destination sessions on a switch must use the same IP address. You enter the ip address command to configure the IP address for the ERSPAN destination sessions. If the ERSPAN destination IP address is not a Supervisor Engine 720 (for example, it is a network sniffer), the traffic arrives with the GRE and RSPAN headers/encapsulation intact.

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You configure the same address in both the source and destination sessions with the ip address command.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The local ERSPAN session limits are as follows:
- Total sessions--66
- Source sessions--2 (ingress or egress or both)
- Destination sessions--23

The monitor session type command creates a new ERSPAN session or allows you to enter the ERSPAN session configuration mode. ERSPAN uses separate source and destination sessions. You configure the source and destination sessions on different switches. The ERSPAN session configuration mode prompts are as follows:
- Router(config-mon-erspan-src)--Indicates the ERSPAN source session configuration mode.
• Router(config-mon-erspan-src-dst)--Indicates the ERSPAN source session destination configuration mode.

• Router(config-mon-erspan-dst)--Indicates the ERSPAN destination session configuration mode.

• Router(config-mon-erspan-dst-src)--Indicates the ERSPAN destination session source configuration mode

The table below lists the ERSPAN destination session configuration mode syntaxes.

**Table 30: ERSPAN Destination Session Configuration Mode Syntaxes**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Configuration Mode</strong></td>
<td></td>
</tr>
<tr>
<td>monitor session erspan-destination-session-number</td>
<td>Enters ERSPAN or RSPAN destination session configuration mode and changes the prompt to the following: Router(config-mon-erspan-dst)# Router(config-mon-rspan-dst)#</td>
</tr>
<tr>
<td>erspan-destination</td>
<td></td>
</tr>
<tr>
<td>rspan-destination</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Session Configuration Mode</td>
<td></td>
</tr>
<tr>
<td>description session-description</td>
<td>(Optional) Describes the ERSPAN or RSPAN destination session.</td>
</tr>
<tr>
<td>shutdown</td>
<td>(Optional) (Default) Inactivates the ERSPAN destination session.</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Activates the ERSPAN destination session.</td>
</tr>
<tr>
<td>destination {single-interface</td>
<td>interface-list</td>
</tr>
<tr>
<td>source</td>
<td>Enters ERSPAN destination session source configuration mode and changes the prompt to the following: Router(config-mon-erspan-dst-src)#</td>
</tr>
<tr>
<td>Destination Session Source Configuration Mode</td>
<td></td>
</tr>
<tr>
<td>ip address ip-address [force]</td>
<td>Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.</td>
</tr>
<tr>
<td>erspan-id erspan-flow-id</td>
<td>Configures the ID number used by the destination and destination sessions to identify the ERSPAN traffic.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Configures the VRF name of the packets in the ERSPAN traffic.</td>
</tr>
</tbody>
</table>

The table below lists the ERSPAN source session configuration mode syntaxes.
### Table 31: ERSPAN or RSPAN Source Session Configuration Mode Syntaxes

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Configuration Mode</strong></td>
<td></td>
</tr>
<tr>
<td><code>monitor session erspan-source-session-number type</code></td>
<td>Enters ERSPAN or RSPAN source session configuration mode and changes the</td>
</tr>
<tr>
<td>`erspan-source</td>
<td>rspan-source`</td>
</tr>
<tr>
<td>Router(config-mon-erspan-src)#</td>
<td></td>
</tr>
<tr>
<td>Router(config-mon-rspan-src)#</td>
<td></td>
</tr>
<tr>
<td><strong>Source Session Configuration Mode</strong></td>
<td></td>
</tr>
<tr>
<td><code>description session-description</code></td>
<td>(Optional) Describes the ERSPAN or RSPAN source session.</td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>(Optional) (Default) Inactivates the ERSPAN or RSPAN source session.</td>
</tr>
<tr>
<td><code>no shutdown</code></td>
<td>Activates the ERSPAN or RSPAN source session.</td>
</tr>
<tr>
<td><code>source</code> {{single-interface</td>
<td>interface-list</td>
</tr>
<tr>
<td></td>
<td>ports or VLANs, and selects the traffic direction to be monitored.</td>
</tr>
<tr>
<td><code>filter</code> {{single-vlan</td>
<td>vlan-list</td>
</tr>
<tr>
<td></td>
<td>source is a trunk port.</td>
</tr>
<tr>
<td><code>description session-description</code></td>
<td>(Optional) Describes the ERSPAN or RSPAN source session.</td>
</tr>
<tr>
<td><strong>Source Session Destination Configuration Mode</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip address ip-address</code></td>
<td>Configures the ERSPAN or RSPAN flow destination IP address, which must</td>
</tr>
<tr>
<td></td>
<td>also be configured on an interface on the destination switch and be entered</td>
</tr>
<tr>
<td></td>
<td>in the ERSPAN or RSPAN destination session configuration.</td>
</tr>
<tr>
<td><code>erspan-id erspan-flow-id</code></td>
<td>Configures the ID number used by the source and destination sessions to</td>
</tr>
<tr>
<td></td>
<td>identify the ERSPAN or RSPAN traffic.</td>
</tr>
<tr>
<td><code>origin ip address ip-address</code></td>
<td>Configures the IP address used as the source of the ERSPAN or RSPAN</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td><code>ip</code> {{ttl ttl-value }</td>
<td>{precipp-value }</td>
</tr>
<tr>
<td></td>
<td>traffic:</td>
</tr>
<tr>
<td></td>
<td>• <code>ttl ttl-value</code> --IP time-to-live (TTL) value</td>
</tr>
<tr>
<td></td>
<td>• <code>prec ipp-value</code> -- IP-precedence value</td>
</tr>
<tr>
<td></td>
<td>• <code>dscp dscp-value</code> -- IP-precedence value</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Configures the VRF name of the packets in the ERSPAN or RSPAN</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
</tbody>
</table>

When you configure the monitor sessions, follow these syntax guidelines:
• erspan-destination-span-session-number can range from 1 to 66.
• single-interface is interface type slot /port ; type is fastethernet, gigabitethernet, or tengigabitethernet.
• interface-list is single-interface , single-interface , single-interface ...

Note
In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

• interface-range is interface type slot /first-port - last-port .
• mixed-interface-list is, in any order, single-interface , interface-range , ...
• erspan-flow-id can range from 1 to 1023.

When you clear the monitor sessions, follow these syntax guidelines:
• The no monitor session session-number command entered with no other parameters clears the session session-number .
• session-range is first-session-number -last-session-number.

Note
When you enter the no monitor session range command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

Use the monitor session type local command to configure ingress, egress, or both ingress and egress SPAN sessions.

Use the monitor session type local-tx command to configure egress-only SPAN sessions.

When you enter the local or the local egress-only SPAN session configuration mode, the prompt changes accordingly to Router(config-mon-local)# or Router(config-mon-local-tx)#, and the following commands are available:

• description -- Describes the properties for this session using this syntax:

description  description

The description can be up to 240 characters and cannot contain special characters or spaces.

• destination -- Specifies the destination and the destination properties using this syntax:

destination  analysis-module  num  anomaly-detector-module  num  interface  type  number
intrusion-detection-module  num

<table>
<thead>
<tr>
<th>analysis-module  num</th>
<th>Specifies the SPAN destination analysis-module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>anomaly-detector-module  num</td>
<td>Specifies the SPAN destination anomaly-detector-module.</td>
</tr>
</tbody>
</table>
### interface type number

Specifies the **interface** type and **number** as follows:

- **GigabitEthernet** `mod/port`
- **port-channel** `num` -- Ethernet Channel of interfaces; valid values are from 1 to 496.

### ingress

(Optional) Configures destinations to receive traffic from attached devices.

### learning

(Optional) Enables MAC address learning from the destinations, which allows the switch to transmit traffic that is addressed to devices attached to the destinations.

### intrusion-detection-module num

Specifies the SPAN destination intrusion-detection-module.

- **exit** -- Exits from configuration session mode.
- **filter vlan vlan-id** -- Limits the SPAN source traffic to specific VLANs; valid values are from 1 to 4096.
- **no** -- Negates a command or sets its defaults.
- **shutdown** -- Shuts down this session
- **source** -- Specifies the SPAN source interface or VLAN using the following syntax:

<table>
<thead>
<tr>
<th>cpu rp</th>
<th>Associates the local SPAN session number with the CPU on the route processor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu sp</td>
<td>Associates the local SPAN session number with the CPU on the switch processor.</td>
</tr>
</tbody>
</table>

### interface type number

Specifies the interface type and number as follows:

- **FastEthernet** `mod/port`
- **GigabitEthernet** `mod/port`
- **Port-channel** `num` -- Ethernet Channel of interfaces; valid values are from 1 to 496.

### vlan vlan-id

Specifies the VLAN; valid values are from 1 to 4094.

| , | (Optional) Specifies another range of interfaces. |
| - | (Optional) Specifies a range of interfaces. |
| both | (Optional) Monitors the received and the transmitted traffic. |
| rx | (Optional) Monitors the received traffic only. |
**tx** When you enter the local-tx keyword, the rx and both keywords are not available and the tx keyword is required.

(Optional) Monitors the transmitted traffic only.

The local SPAN session limits are as follows:

- Total sessions--80
- Source sessions--2 (ingress or egress or both)
- Egress only--14

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

Only one destination per SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

You can configure up to 64 SPAN destination interfaces, but you can have one egress SPAN source interface and up to 128 ingress source interfaces only.

A SPAN session can either monitor VLANs or monitor individual interfaces, but it cannot monitor both specific interfaces and specific VLANs. Configuring a SPAN session with a source interface and then trying to add a source VLAN to the same SPAN session causes an error. Configuring a SPAN session with a source VLAN and then trying to add a source interface to that session also causes an error. You must first clear any sources for a SPAN session before switching to another type of source.

Port channel interfaces display in the list of interface options if you have them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session session sourcevlan vlan-id** command.

When you configure the **destination**, use these guidelines:

- A **single-interface** is as follows:
  - interface type slot/port; type is fastethernet, gigabitethernet, or tengigabitethernet.
  - interface port-channel number

**Note**

Destination port channel interfaces must be configured with the **channel-group group-num mode on** command and the **no channel-protocol** command.

- An **interface-list** is single-interface, single-interface , single-interface ...

**Note**

In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- An **interface-range** is interface type slot / first-port - last-port.
- A **mixed-interface-list** is, in any order, single-interface , interface-range , ...
• A single-vlan is the ID number of a single VLAN.
• A single-list is single-vlan, single-vlan, single-vlan ...
• A vlan-range is first-vlan-ID - last-vlan-ID.
• A mixed-vlan-list is, in any order, single-vlan, vlan-range, ...

When you clear the monitor sessions, follow these syntax guidelines:

• The no monitor session session-number command entered with no other parameters clears the session session-number.
• session-range is first-session-number -last-session-number.

---

**Note**

When you enter the no monitor session range command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

---

**Examples**

This example shows how to configure an ERSPAN source session number and enter the ERSPAN source session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-source
```

This example shows how to configure an ERSPAN destination session number and enter the ERSPAN destination session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-destination
```

This example shows how to associate the ERSPAN destination session number with the destination ports:

```
Router(config-mon-erspan-dst)# destination interface fastethernet 1/2, 2/3
```

This example shows how to enter the ERSPAN destination session source configuration:

```
Router(config-mon-erspan-dst)# source
```

This example shows how to enter the ERSPAN destination session source configuration mode:

```
Router(config-mon-erspan-dst)# source
```

This example shows how to configure multiple sources for a session:

```
Router(config-mon-erspan-src)# source interface fastethernet 5/15, 7/3 rx
Router(config-mon-erspan-src)# source interface gigabitethernet 1/2 tx
Router(config-mon-erspan-src)# source interface port-channel 102
Router(config-mon-erspan-src)# source filter vlan 2 - 3
```
This example shows how to enter the ERSPAN source session destination configuration mode:

Router(config-mon-erspan-src)# destination

This example shows how to configure the ID number that is used by the source and destination sessions to identify the ERSPAN traffic:

Router(config-mon-erspan-src-dst)# erspan-id 1005

This example shows how to configure session 1 to monitor ingress traffic from Gigabit Ethernet port 1/1 and configure Gigabit Ethernet port 1/2 as the destination:

Router(config)# monitor session 1 type local
Router(config-mon-local)# source interface gigabitethernet 1/1 rx
Router(config-mon-local)# destination interface gigabitethernet 1/2

This example shows how to configure session 1 to monitor egress-only traffic from Gigabit Ethernet port 5/1 and configure Gigabit Ethernet port 5/2 as the destination:

Router(config)# monitor session 1 type local-tx
Router(config-mon-local)# source interface gigabitethernet 5/1 rx
Router(config-mon-local)# destination interface gigabitethernet 5/2

This example shows how to remove an interface from a session:

Router(config)# no monitor session 1 type local-tx

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session type</td>
<td>Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.</td>
</tr>
<tr>
<td>show monitor session</td>
<td>Displays information about the ERSPAN, SPAN, and RSPAN sessions.</td>
</tr>
</tbody>
</table>

### mop device-code

To identify the type of device sending Maintenance Operation Protocol (MOP) System Identification (sysid) messages and request program messages, use the `mop device-code` command in global configuration mode. To set the identity to the default value, use the `no` form of this command.

`mop device-code` command

```
mop device-code {cisco|ds200}
no mop device-code {cisco|ds200}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco</td>
<td>Denotes a Cisco device code. This is the default.</td>
</tr>
<tr>
<td>ds200</td>
<td>Denotes a DECserver 200 device code.</td>
</tr>
</tbody>
</table>

### Command Default

Cisco device code
mop retransmit-timer

To configure the length of time that the Cisco IOS software waits before resending boot requests to a Maintenance Operation Protocol (MOP) server, use the mop retransmit-timer command in global configuration mode. To reinstate the default value, use the no form of this command.

```
mop retransmit-timer seconds
no mop retransmit-timer
```

**Syntax Description**

| seconds | Sets the length of time (in seconds) that the software waits before resending a message. The value is a number from 1 to 20. |

**Command Default**

4 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, when the software sends a request that requires a response from a MOP boot server and the server does not respond, the message is re-sent after 4 seconds. If the MOP boot server and router are separated by a slow serial link, it might take longer than 4 seconds for the software to receive a response to its message. Therefore, you might want to configure the software to wait longer than 4 seconds before resending the message if you are using such a link.
Examples

In the following example, if the MOP boot server does not respond within 10 seconds after the router sends a message, the server will resend the message:

```
mop retransmit-timer 10
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mop device-code</strong></td>
<td>Identifies the type of device sending MOP sysid messages and requests program messages.</td>
</tr>
<tr>
<td><strong>mop enabled</strong></td>
<td>Enables an interface to support the MOP.</td>
</tr>
</tbody>
</table>

### mop retries

To configure the number of times the Cisco IOS software will resend boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retries** command in global configuration mode. To reinstate the default value, use the **no** form of this command.

```
mop retries count
no mop retries
```

#### Syntax Description

<table>
<thead>
<tr>
<th>count</th>
<th>Indicates the number of times the software will resend a MOP boot request. The value is a number from 3 to 24. The default is 8.</th>
</tr>
</thead>
</table>

#### Command Default

8 times

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Examples

In the following example, the software will attempt to resend a message to an unresponsive host 11 times before declaring a failure:

```
Router(config)# mop retries 11
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mop device-code</strong></td>
<td>Identifies the type of device sending MOP sysid messages and requests program messages.</td>
</tr>
<tr>
<td><strong>mop enabled</strong></td>
<td>Enables an interface to support the MOP server.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mop retransmit-timer</td>
<td>Configures the length of time that the Cisco IOS software waits before resending boot requests to a MOP server.</td>
</tr>
</tbody>
</table>

### more

To display the contents of a file, use the **more** command in privileged EXEC mode.

```
more [ {'/ascii'/binary'/compressed'/ebcdic'} ] url
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ascii</td>
<td>(Optional) Displays a binary file in ASCII format.</td>
</tr>
<tr>
<td>/binary</td>
<td>(Optional) Displays a file in hex/text format.</td>
</tr>
<tr>
<td>/compressed</td>
<td>(Optional) Displays a compressed file in readable format.</td>
</tr>
<tr>
<td>/ebcdic</td>
<td>(Optional) Displays a binary file in EBCDIC format.</td>
</tr>
<tr>
<td>url</td>
<td>The URL of the file to display. A URL in the CLI consists of a file-system prefix (such as system: or nvram:), an optional path (such as a folder name), and the name of a file.</td>
</tr>
</tbody>
</table>

**Command Default**

The command displays the content of a file in its native format. Optional formats include ascii, binary, compressed, and ebcDIC.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE 2.5</td>
<td>This command was integrated into Cisco IOS XE Release 2.5 on ASR 1000 series devices.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.13S</td>
<td>This command was modified. The /compressed keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `more system:running-config` command displays the same output as the `show running-config` command. The `more nvram:startup-config` command is recommended as a replacement for the `show startup-config` command and the `show configuration` command.

You can use the following commands to display configuration files:

- The `more nvram:startup-config` command displays the startup configuration file that is contained in NVRAM or specified by the CONFIG_FILE environment variable. The Cisco IOS software informs you whether the displayed configuration is a complete configuration or a distilled version. A distilled configuration is one that does not contain access lists.

- The `more system:running-config` command displays the running configuration.
These commands show the version number of the software used when you last changed the configuration file. You can also display the contents of files on remote systems using the `more` command. For example, you could display a saved running configuration file on an FTP server using `more ftp://username:password@ftp-host1/mydirectory/7200-basic-running-config`. See the description of the `copy` command for more information on file-system prefixes available in the Cisco IOS CLI.

Options for filtering and redirecting the output of this command are available by appending a pipe character (`|`). See the Related Commands table for a list of `more <url>` command extensions.

**Examples**

The following partial sample output displays the configuration file named startup-config in NVRAM:

```
Router# more nvram:startup-config
!
! No configuration change since last restart
! NVRAM config last updated at 02:03:26 PDT Thu Oct 2 1997
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service udp-small-servers
service tcp-small-servers
.
.
end
```

The following is partial sample output from the `more nvram:startup-config` command when the configuration file has been compressed:

```
Router#
more nvram:startup-config

Using 21542 out of 65536 bytes, uncompressed size = 142085 bytes
!
version 12.1
service compress-config
!
hostname rose
!
.
.
```

The following partial sample output displays the running configuration:

```
Router2# more system:running-config

Building configuration...
Current configuration:
!
version 12.1
no service udp-small-servers
no service tcp-small-servers
!
hostname Router2
!
.
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).</td>
</tr>
<tr>
<td>more &lt;url&gt; begin</td>
<td>Begins the output of any more command from a matched string.</td>
</tr>
<tr>
<td>more &lt;url&gt; exclude</td>
<td>Filters the output of any more command to exclude a matched string.</td>
</tr>
<tr>
<td>more &lt;url&gt; include</td>
<td>Filters the output of any more command to display only the lines that match the specified string.</td>
</tr>
<tr>
<td>service compress-config</td>
<td>Compresses startup configuration files.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
</tr>
</tbody>
</table>

**more url begin**

To search the output of any more command, use the more url | begin command in EXEC mode. This command begins unfiltered output of the more command with the first line that contains the regular expression you specify.

```
{more url|begin regular-expression}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>url</th>
<th>The Universal Resource Locator (RLl) of the file to display. More commands are advanced show commands; for details, see the command reference page in this book for the more command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.</td>
</tr>
<tr>
<td>regular-expression</td>
<td>Any regular expression found in more command output.</td>
</tr>
<tr>
<td>/</td>
<td>Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.</td>
</tr>
<tr>
<td>-</td>
<td>Specifies a filter at a --More-- prompt that only displays output lines that do not contain the regular expression.</td>
</tr>
<tr>
<td>+</td>
<td>Specifies a filter at a --More-- prompt that only displays output lines that contain the regular expression.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC
Privileged EXEC
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>The <strong>more</strong> command was introduced.</td>
</tr>
<tr>
<td>12.0(1)T</td>
<td>This extension of the <strong>more</strong> command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

You can specify a new search at every **More** prompt.

To search the remaining output of the **more** command, use the following command at the **More** prompt:

```
/ regular-expression
```

To filter the remaining output of the **more** command, use one of the following commands at the **More** prompt:

- **regular-expression**
- **regular-expression**
- **regular-expression**

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl-^** (Ctrl-Shift-6) or **Ctrl-Z**.

### Note

Once you specify a filter for a **more** command, you cannot specify another filter at a **More** prompt. The first specified filter remains until the **more** command output finishes or until you interrupt the output. The use of the keyword **begin** does not constitute a filter.

Because prior output is not saved, you cannot search or filter backward through prior output.

### Examples

The following is partial sample output of the **more nvram:startup-config | begin ip** command that begins unfiltered output with the first line that contain the regular expression “ip.” At the **More** prompt, the user specifies a filter to exclude output lines that contain the regular expression “ip.”

```
router# more nvram:startup-config | begin ip
ip subnet-zero
ip domain-name cisco.com
ip name-server 198.92.30.32
ip name-server 171.69.2.132
!
isdn switch-type primary-5ess
.
.
interface Ethernet1
  ip address 5.5.5.99 255.255.255.0
--More--
  -ip
  filtering...
  media-type 10BaseT
  !
interface Serial0:23
  encapsulation frame-relay
  no keepalive
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>more &lt;url&gt; exclude</td>
<td>Filters more command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>more &lt;url&gt; include</td>
<td>Filters more command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>show &lt;command&gt; begin</td>
<td>Searches the output of any show command and displays the output from the first instance of a specified string.</td>
</tr>
<tr>
<td>show &lt;command&gt; exclude</td>
<td>Filters show command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>show &lt;command&gt; include</td>
<td>Filters show command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
</tbody>
</table>

more url exclude

To filter more command output so that it excludes lines that contain a particular regular expression, use the more exclude command in EXEC mode.

\{more url|exclude regular-expression\}

Syntax Description

<table>
<thead>
<tr>
<th>url</th>
<th>The Universal Resource Locator (URL) of the file to display. More commands are advanced show commands; for details, see the command reference page in this book for the more command. The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include: prefix:[directory]/filename Prefixes can be local file systems or file locations, such as nvram: or system:. Alternatively, you can specify network locations using the following syntax: ftp: [[[\username: \password[@]]location ]/directory ]/filename tftp: [[/location ]/directory ]/filename rcp: [[/\username[@]]location ]/directory ]/filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>regular-expression</td>
<td>Any regular expression found in more command output.</td>
</tr>
<tr>
<td>/</td>
<td>Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.</td>
</tr>
</tbody>
</table>
The `more` command was introduced. 11.3 AA
This extension of the `more` command was introduced. 12.0(1)T
This command was integrated into Cisco IOS Release 12.2(33)SRA.

The `regular-expression` argument is case sensitive and allows for complex matching requirements.

You can specify a new search at any --More-- prompt. To search the remaining output of the `more` command, use the following command at the --More-- prompt:

```
/ regular-expression
```

When output volume is large, the search can produce long lists of output. To interrupt the output, press Ctrl-^ (Ctrl-Shift-6) or Ctrl-Z.

Because prior output is not saved, you cannot search or filter backward through prior output.

The following is partial sample output of the `more nvram:startup-config | exclude service` command. The use of `| exclude service` in the command specifies a filter that excludes lines that contain the regular expression “service.” At the --More-- prompt, the user searches for the regular expression “Dialer1,” which continues filtered output with the first line that contains “Dialer1.”

```
router# more nvram:startup-config | exclude service
!
version 12.0
!
hostname router
!
boot system flash
no logging buffered
!
ip subnet-zero
ip domain-name cisco.com
.
.
--More--
/Dialer1
filtering...
interface Dialer1
no ip address
no ip directed-broadcast
dialer in-band
no cdp enable
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>more &lt;url&gt; begin</code></td>
<td>Begins unfiltered output of the <code>more</code> command with the first line that contains the regular expression you specify.</td>
</tr>
</tbody>
</table>
more url include

To filter more command output so that it displays only lines that contain a particular regular expression, use the more include command in EXEC mode.

```bash
{more url include regular-expression}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>url</code></td>
<td>The Universal Resource Locator (URL) of the file to display. More commands are advanced show commands; for details, see the command reference page in this book for the more command.</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td><code>regular-expression</code></td>
<td>Any regular expression found in more command output.</td>
</tr>
<tr>
<td><code>/</code></td>
<td>Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.</td>
</tr>
</tbody>
</table>

### Command Modes

**EXEC**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>The more command was introduced.</td>
</tr>
<tr>
<td>12.0(1)T</td>
<td>This extension of the more command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The regular-expression argument is case sensitive and allows for complex matching requirements.

You can specify a new search at any --More-- prompt. To search the remaining output of the more command, use the following syntax at the --More-- prompt:

```
/ regular-expression
```

When output volume is large, the search can produce long lists of output. To interrupt the output, press Ctrl-^ (Ctrl-Shift-6) or Ctrl-Z.
Because prior output is not saved, you cannot search or filter backward through prior output.

**Examples**

The following is partial sample output of the `more nvram:startup-config | include ip` command. It only displays lines that contain the regular expression “ip.”

```
router# more nvram:startup-config | include ip
ip subnet-zero
ip domain-name cisco.com
ip name-server 198.92.30.32
ip name-server 171.69.2.132
description ip address 172.21.53.199 255.255.255.0
ip address 172.21.53.199 255.255.255.0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>more &lt;url&gt; begin</code></td>
<td>Begins unfiltered output of the <code>more</code> command with the first line that contains the regular expression you specify.</td>
</tr>
<tr>
<td><code>more &lt;url&gt; exclude</code></td>
<td>Filters <code>more</code> command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; begin</code></td>
<td>Searches the output of any <code>show</code> command and displays the output from the first instance of a specified string.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; exclude</code></td>
<td>Filters <code>show</code> command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; include</code></td>
<td>Filters <code>show</code> command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
</tbody>
</table>

**more flh:logfile**

To view the system console output generated during the Flash load helper operation, use the `more flh:logfile` privileged EXEC command.

```
more flh:logfile
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you are a remote Telnet user performing the Flash upgrade without a console connection, this command allows you to retrieve console output when your Telnet connection has terminated due to the switch to the
ROM image. The output indicates what happened during the download, and is particularly useful if the download fails.

This command is a form of the `more` command. See the `more` command for more information.

**Examples**

The following is sample output from the `more flh:logfile` command:

```
Router# more flh:logfile
%FLH: abc/igs-kf.914 from 172.16.1.111 to flash...
System flash directory:
File
Length Name/status
1 2251320
abc/igs-kf.914
[2251384 bytes used, 1942920 available, 4194304 total]
Accessing file 'abc/igs-kf.914' on 172.16.1.111...
Loading from 172.16.13.111:
Erasing device...... erased
Loading from 172.16.13.111:
- [OK = 2251320/4194304 bytes]
Verifying checksum... OK (0x97FA)
Flash copy took 79292 msecs
%FLH: Re-booting system after download
Loading abc/igs-kf.914 at 0x3000040, size = 2251320 bytes [OK]
F3: 2183364+67924+259584 at 0x3000060
```

Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134

Cisco Internetwork Operating System Software
Cisco IOS (tm) GS Software (GS7), Version 11.0
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 06-Dec-94 14:01 by smith
Image text-base: 0x00001000, data-base: 0x005A9C94
cisco 2500 (68030) processor (revision 0x0) with 4092K/2048K bytes of memory.
Processor board serial number 00000000
DDN X.25 software, Version 2.0, NET2 and BFE compliant.
ISDN software, Version 1.0.
Bridging software.
Enterprise software set supported. (0x0)
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
--More--
1 ISDN Basic Rate interface.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read ONLY)
motd-banner

To enable the display of message-of-the-day (MOTD) banners on the specified line or lines, use the `motd-banner` command in line configuration mode. To suppress the MOTD banners on the specified line or lines, use the `no` form of this command.

```
motd-banner
no motd-banner
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Enabled on all lines.

**Command Modes**
Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command determines whether the router will display the MOTD banner when an EXEC session is created on the specified line or lines. The MOTD banner is defined with the `banner motd` global configuration command. By default, the MOTD banner is enabled on all lines. Disable the MOTD banner on specific lines using the `no motd-banner` line configuration command.

The MOTD banners can also be disabled by the `no exec-banner` line configuration command, which disables both MOTD banners and EXEC banners on a line. If the `no exec-banner` command is configured on a line, the MOTD banner will be disabled regardless of whether the `motd-banner` command is enabled or disabled. The table below summarizes the effects of the `exec-banner` command and the `motd-banner` command.

**Table 32: Banners Displayed Based On exec-banner and motd-banner Combinations**

<table>
<thead>
<tr>
<th></th>
<th>exec-banner (default)</th>
<th>no exec-banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>motd-banner (default)</td>
<td>MOTD banner</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>EXEC banner</td>
<td></td>
</tr>
<tr>
<td>no motd-banner</td>
<td>EXEC banner</td>
<td>None</td>
</tr>
</tbody>
</table>

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the `no exec-banner` command or `no motd-banner` command is configured. The table below summarizes the effects of the `exec-banner` command and the `motd-banner` command for reverse Telnet connections.

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>more</td>
<td>Displays a file.</td>
</tr>
</tbody>
</table>
Table 33: Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines

<table>
<thead>
<tr>
<th>exec-banner (default)</th>
<th>no exec-banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>motd-banner (default)</td>
<td>MOTD banner</td>
</tr>
<tr>
<td></td>
<td>Incoming banner</td>
</tr>
<tr>
<td>no motd-banner</td>
<td>Incoming banner</td>
</tr>
</tbody>
</table>

Examples

The following example suppresses the MOTD banner on vty lines 0 through 4:

```
line vty 0 4
no motd-banner
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>banner exec</strong></td>
<td>Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.</td>
</tr>
<tr>
<td><strong>banner incoming</strong></td>
<td>Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.</td>
</tr>
<tr>
<td><strong>banner motd</strong></td>
<td>Defines and enables a customized message-of-the-day banner.</td>
</tr>
<tr>
<td><strong>motd-banner</strong></td>
<td>Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.</td>
</tr>
</tbody>
</table>

name-connection

To assign a logical name to a connection, use the `name-connection` command in user EXEC mode.

```
name-connection
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No logical name is defined.

**Command Modes**

User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can be useful for keeping track of multiple connections. You are prompted for the connection number and name to assign. The `where` command displays a list of the assigned logical connection names.
Examples

The following example assigns the logical name blue to the connection:

```
Router> where
Conn Host Address    Byte  Idle Conn Name
  * 1 doc-2509 172.30.162.131  0  0  doc-2509
```

```
Router> name-connection
Connection number: 1
Enter logical name:
blue
Connection 1 to doc-2509 will be named "BLUE" [confirm]
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>where</td>
<td>Lists open sessions associated with the current terminal line.</td>
</tr>
</tbody>
</table>

nmsp enable

To enable Network Mobility Service Protocol (NMSP) features on the device, use the `nmsp enable` command in global configuration mode. To disable, use the `no` form of this command.

```
nmsp enable
no nmsp enable
```

Syntax Description

This command has no arguments or keywords.

Command Default

NMSP features are not enabled.

Command Modes

Global configuration (config)

Command History

- **Release**: 15.2(2)E
- **Modification**: This command was introduced.

Usage Guidelines

Configuring the `nmsp enable` command enables NMSP features on the switch. However, configuring the `nmsp stong-cipher` command before enabling the NMSP features ensures that all NMSP connections use strong ciphers.

Examples

The following example shows how to enable NMSP features:

```
Device> enable
Device> configure terminal
Device(config)# nmsp enable
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show nmsp status</td>
<td>Displays the status of active NMSP connections.</td>
</tr>
</tbody>
</table>
nmsp strong-cipher

To enable the new ciphers, use the `nmsp strong-cipher` command in global configuration mode. To disable, use the `no` form of this command.

```
nmsp strong-cipher
no nmsp strong-cipher
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

The new ciphers are not enabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `nmsp strong-cipher` command enables strong ciphers for new Network Mobility Service Protocol (NMSP) connections.

**Note**

The existing NMSP connections will use the default cipher.

### Examples

The following example shows how to enable a strong-cipher for NMSP:

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show nmsp status</code></td>
<td>Displays the status of active NMSP connections.</td>
</tr>
</tbody>
</table>

**no menu**

To delete a user menu from the configuration file, use the `no menu` command in global configuration mode.

```
no menu menu-name
```

### Syntax Description

| menu-name | Name of the menu to delete from the configuration file. |

### Command Default

No default behavior or values.
**notify**

To enable terminal notification about pending output from other Telnet connections, use the `notify` command in line configuration mode. To disable notifications, use the `no notify` form of this command.

```
notify
no notify
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command sets a line to inform a user that has multiple, concurrent Telnet connections when output is pending on a connection other than the current one.

Examples

In the following example, notification of pending output from connections is enabled on virtual terminal lines 0 to 4:

Router(config)# line vty 0 4
Router(config-line)# notify

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal notify</td>
<td>Configures a line to inform a user that has multiple, concurrent Telnet connections when output is pending on a connection other than the current one.</td>
</tr>
</tbody>
</table>

**notify syslog**

To enable the sending of notifications of configuration changes to a remote system message logging (syslog), use the `notify syslog` command in configuration change logger configuration mode. To disable the sending of notifications of configuration changes to the syslog, use the `no notify syslog` form of this command.

```
notify syslog [contenttype {plaintext|xml}]
no notify syslog [contenttype {plaintext|xml}]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contenttype</td>
<td>(Optional) Allows you to choose a format for the configuration change messages that are sent via syslog.</td>
</tr>
<tr>
<td>plaintext</td>
<td>(Optional) Specifies that the configuration change messages are sent as plain text.</td>
</tr>
<tr>
<td>xml</td>
<td>(Optional) Specifies that the configuration change messages are sent in XML format.</td>
</tr>
</tbody>
</table>

Command Default

Notifications are not sent to the syslog.

Command Modes

Configuration change logger configuration (config-archive-log-config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>The <code>contenttype plaintext</code>, and <code>xml</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>
Enable the **notify syslog** command if you use the syslog to monitor your device. Syslog monitoring prevents the need to gather configuration log information manually.

**Note**

When a system message contains lengthy descriptive information, the message text can sometimes exceed the syslog buffer. In releases earlier than Cisco IOS Release 12.2(33)SXF2, the overrun message is truncated to the buffer size and any additional text is lost.

In Cisco IOS Release 12.2(33)SXF2 and later releases, a long message can be split into multiple messages, with truncation and continuation indicators at each section. The end of an incomplete syslog message section will be tagged with the string "***MSG XXXXX TRUNCATED***", where XXXXX is a count of overrun messages since the last system reload. The continuation of the message will begin with "***MSG XXXXX CONTINUATION #YY", where YY represents the part number. A message can be divided into a maximum of 99 parts. When truncation occurs, the following message is sent after the truncated message:

%Log packet overrun, PC [hex], format: [chars]

**Examples**

The following example shows how to enable the device to send notifications (in XML format) to the syslog:

```
Device# configure terminal
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# notify syslog contenttype xml
Device(config-archive-log-config)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td>hidekeys</td>
<td>Suppresses the display of password information in configuration log files.</td>
</tr>
<tr>
<td>log config</td>
<td>Enters configuration change logger configuration mode.</td>
</tr>
<tr>
<td>logging enable</td>
<td>Enables the logging of configuration changes.</td>
</tr>
<tr>
<td>logging size</td>
<td>Specifies the maximum number of entries retained in the configuration log.</td>
</tr>
<tr>
<td>show archive log config</td>
<td>Displays entries from the configuration log.</td>
</tr>
</tbody>
</table>

**padding**

To set the padding on a specific output character, use the **padding** command in line configuration mode. To remove padding for the specified output character, use the **no** form of this command.

```
padding ascii-number count
no padding ascii-number
```

**Syntax Description**

| ascii-number | ACII decimal representation of the character. |
| count | Number of NULL bytes sent after the specified character, up to 255 padding characters in length. |

**Command Default**
No padding

**Command Modes**
Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command when the attached device is an old terminal that requires padding after certain characters (such as ones that scrolled or moved the carriage). See the “ASCII Character Set and Hex Values” appendix for a list of ASCII characters.

**Examples**
In the following example, the Return (decimal character 13) is padded with 25 NULL bytes on the console line:

```
Router(config)# line console
Router(config-line)# padding 13 25
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal padding</td>
<td>Changes the character padding on a specific output character for the current session.</td>
</tr>
</tbody>
</table>

**parity**

To define generation of a parity bit, use the `parity` command in line configuration mode. To specify no parity, use the `no` form of this command.

```
purity {none|even|odd|space|mark}
no  parity
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No parity. This is the default.</td>
</tr>
<tr>
<td>even</td>
<td>Even parity.</td>
</tr>
<tr>
<td>odd</td>
<td>Odd parity.</td>
</tr>
<tr>
<td>space</td>
<td>Space parity.</td>
</tr>
<tr>
<td>mark</td>
<td>Mark parity.</td>
</tr>
</tbody>
</table>

**Command Default**
No parity.
Line configuration

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line configuration</td>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.4</td>
<td>This command was modified to enable parity setting on Cisco AS5350 and Cisco AS5400 NextPort lines.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Communication protocols provided by devices such as terminals and modems sometimes require a specific parity bit setting. Refer to the documentation for your device to determine required parity settings.

If you use this command to set parity on Cisco AS5350 and Cisco AS5400 NextPort lines, do not also set parity by means of S-register settings in a modemcap. (A modemcap is a series of parameter settings that are sent to your modem to configure it to interact with a Cisco device in a specified way. Cisco IOS software defines modemcaps that have been found to properly initialize most modems so that they function properly with Cisco routers and access servers.)

Examples

In the following example, even parity is configured for line 34:

```
Router(config)# line 34
Router(config-line)# parity even
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal parity</td>
<td>Defines the generation of the parity bit for the current for the current session and line.</td>
</tr>
</tbody>
</table>

**parser cache**

To reenable the Cisco software parser cache after disabling it, use the `parser cache` command in global configuration mode. To disable the parser cache, use the `no` form of this command.

```
parser cache
no parser cache
```

Syntax Description

This command has no arguments or keywords.

Command Default

Parser cache is enabled by default.

Command Modes

Global configuration (config)

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.1(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
The Parser Cache feature optimizes the parsing (translation and execution) of Cisco software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.

The parser cache is enabled by default. However, if you wish to disable the parser cache, you may do so using the `no parser cache` command in global configuration mode. To reenable the parser cache after it has been disabled, use the `parser cache` command.

When the `no parser cache` is issued, the command line appears in the running configuration file. However, if the parser cache is reenabled, no command line appears in the running configuration file.

In the following example, the Parser Cache feature is disabled:

```
Device(config)# no parser cache
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear parser cache</code></td>
<td>Clears the parse cache entries and hit/miss statistics stored for the Parser Cache feature.</td>
</tr>
<tr>
<td><code>show parser statistics</code></td>
<td>Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.</td>
</tr>
</tbody>
</table>

### parser command serializer

To enable configuration access only to the users holding a configuration lock and to prevent other clients from accessing the running configuration, use the `parser command serializer` command in global configuration mode. To disable this configuration, use the `no` form of this command.

```
parser command serializer
no parser command serializer
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Access is granted only to the user holding the lock.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)T</td>
<td>This command was included in Cisco IOS Release 15.1(1)T.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The Parser Concurrency and Locking Improvements feature ensures that exclusive access is granted only to a requested process and prevents other users from concurrently accessing the Cisco IOS configuration. That is, it prevents simultaneous execution of two or more commands. Use the **parser command serializer** command to configure the Parser Concurrency and Locking Improvements feature.

Examples

The following example shows how to configure the Parser Concurrency and Locking Improvements feature:

```
Router# configure terminal
Router(config)# parser command serializer
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configuration mode exclusive</code></td>
<td>Enables single-user (exclusive) access functionality for the Cisco IOS CLI.</td>
</tr>
<tr>
<td><code>configure terminal lock</code></td>
<td>Locks the running configuration into exclusive configuration mode for the duration of your configuration session.</td>
</tr>
<tr>
<td><code>test parser session-lock</code></td>
<td>Tests the behavior of the Parser Concurrency and Locking Improvements feature.</td>
</tr>
</tbody>
</table>

**parser config cache interface**

To reduce the time required for the command-line interpreter to execute commands that manage the running system configuration files, use the **parser config cache interface** command in global configuration mode. To disable the reduced command execution time functionality, use the **no** form of this command.

**parser config cache interface**

**no parser config cache interface**

### Syntax Description

This command has no arguments or keywords.

### Command Default

Disabled

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS XE Release 3.9S.

### Usage Guidelines

Enable the `parser config cache interface` command to reduce the execution time required for running configuration management commands such as the `show running-configuration`, `write terminal`, and `copy system:running-configuration` commands. Information for these configuration management commands is supplied by nonvolatile generation (NVGEN) processes that query the system for configuration details. The `parser config cache interface` command is especially useful for managing large system configurations that contain numerous interface configurations.

Once enabled, the command provides faster execution of the NVGEN commands that process the running system configuration by caching interface configurations in system memory, and by retrieving only configuration information that has changed. For this reason, the device on which this command is enabled must have enough memory available to store the interface configuration. For example, if the interface configurations take up 15 KB of memory, using this command would require having an additional 15 KB of memory space available.

The first time you display the configuration file, you will not see much evidence of improvement in performance because the interface cache will be filled up. However, you will notice performance improvements when you enter subsequent NVGEN-type commands such as the `show running-configuration` EXEC command.

Each time the interface configuration is changed, the interface cache is flushed. Entering an NVGEN-type command after modifying the interface configuration will once again not show any performance improvement until the next NVGEN-type command is entered.

### Examples

The following example shows how to enable the functionality for reducing the time required for the command-line interpreter to execute commands that manage the running system configuration files:

```
Device(config)# parser config cache interface
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy system:running-configuration</code></td>
<td>Copies the running configuration to another destination.</td>
</tr>
<tr>
<td><code>show running-configuration</code></td>
<td>Displays the configuration currently running on the terminal.</td>
</tr>
<tr>
<td><code>write terminal</code></td>
<td>Displays the configuration currently running on the terminal.</td>
</tr>
</tbody>
</table>

### parser config partition

To enable configuration partitioning, use the `parser config partition` command. To disable the partitioning of the running configuration, use the `no` form of this command.

```
parser config partition
no parser config partition
```

### Syntax Description

No arguments or keywords.
This command is enabled by default.

**Command Modes**  
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRB</td>
<td>This command was introduced as part of the Configuration Partitioning feature.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command controls (enables or disables) the Configuration Partitioning feature.

**Note**

This command is not related to disk partitions or disk partitioning.

To display the list of commands that make up the current running configuration for a specific part ("partition") of the system’s global running configuration, use the `show running-config partition` command in privileged Exec mode.

The Configuration Partitioning feature uses a small amount of system resources. The `no parser config partition` command allows you to disable this feature if the feature is not needed on your system.

**Note**

Only the `no` form of this command appears in configuration files. To determine if config partitioning is supported on your system and whether it is enabled, use the `show running-config parser ?` command.

**Examples**

The following example shows how to disable partitioning of the system running configuration:

```
Device> enable
Device# config t

Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no parser config partition
System configured
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config partition</code></td>
<td>Displays the list of commands that make up the current running configuration for a specific part of the system’s global running configuration. When used with the <code>?</code> CLI help keyword, can also be used to determine the availability and status of the Configuration Partitioning feature.</td>
</tr>
</tbody>
</table>
**parser maximum**

To specify performance maximums for CLI operations use the `parser maximum` command in global configuration mode. To clear any previously established maximums, use the `no` form of the command.

```
parser maximum {latency|utilization} limit
no parser maximum {latency|utilization}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>latency</code></td>
<td>Specifies the maximum process latency to allow.</td>
</tr>
<tr>
<td><code>limit</code></td>
<td>Numerical latency between 20 and 200.</td>
</tr>
<tr>
<td><code>utilization</code></td>
<td>Specifies the maximum CPU utilization to allow.</td>
</tr>
<tr>
<td><code>limit</code></td>
<td>Numerical CPU utilization between 1 and 100.</td>
</tr>
</tbody>
</table>

**Command Default**

No performance maximums enabled by default.

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Parser Maximum feature provides a workaround in the event of a problem with the coding of a protocol, allowing the error to be bypassed until it can be corrected.

**Examples**

The following example shows how to impose a latency limit of 100.

```
Router(config)#parser maximum latency 100
```

The following example shows how to clear latency limits.

```
Router(config)#no parser maximum latency
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parser cache</td>
<td>The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.</td>
</tr>
</tbody>
</table>

**partition**

To separate Flash memory into partitions on Class B file system platforms, use the `partition` command in global configuration mode. To undo partitioning and to restore Flash memory to one partition, use the `no` form of this command.
Cisco 1600 Series and Cisco 3600 Series Routers
partition flash-filesystem: [number-of-partitions] [partition-size]
no partition flash-filesystem:

All Other Class B Platforms
partition flash partitions [size1 size2]
no partition flash

Syntax Description

<table>
<thead>
<tr>
<th>flash-filesystem</th>
<th>One of the following Flash file systems, which must be followed by a colon (:). The Cisco 1600 series can only use the flash: keyword.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• flash: -- Internal Flash memory</td>
</tr>
<tr>
<td></td>
<td>• slot0: -- Flash memory card in PCMCIA slot 0</td>
</tr>
<tr>
<td></td>
<td>• slot1: -- Flash memory card in PCMCIA slot 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>number-of-partitions</th>
<th>(Optional) Number of partitions in Flash memory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>partition-size</td>
<td>(Optional) Size of each partition. The number of partition size entries must be equal to the number of specified partitions.</td>
</tr>
<tr>
<td>partitions</td>
<td>Number of partitions in Flash memory. Can be 1 or 2.</td>
</tr>
<tr>
<td>size1</td>
<td>(Optional) Size of the first partition (in megabytes).</td>
</tr>
<tr>
<td>size2</td>
<td>(Optional) Size of the second partition (in megabytes).</td>
</tr>
</tbody>
</table>

Command Default
Flash memory consists of one partition.
If the partition size is not specified, partitions of equal size are created.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines
For the Cisco 1600 series and Cisco 3600 series routers, to undo partitioning, use the partition flash-filesystem :1 or no partition flash-filesystem : command. For other Class B platforms, use either the partition flash 1 or no partition flash command. If there are files in a partition other than the first, you must use the erase flash-filesystem:partition-number command to erase the partition before reverting to a single partition.

When creating two partitions, you must not truncate a file or cause a file to spill over into the second partition.

Note
The partition command will only create 3MB or larger partitions and may not be used if the device memory contains logging persistent files.
**Examples**

The following example creates two partitions of 4 MB each in Flash memory:

```
Router(config)# partition flash 2 4 4
```

The following example divides the Flash memory card in slot 0 into two partitions, each 8 MB in size on a Cisco 3600 series router:

```
Router(config)#
partition slot0: 2 8 8
```

The following example creates four partitions of equal size in the card on a Cisco 1600 series router:

```
Router(config)# partition flash: 4
```

**path (archive configuration)**

To specify the location and filename prefix for the files in the Cisco configuration archive, use the `path` command in archive configuration mode. To disable this function, use the `no` form of this command.

```
path url
no path url
```

**Syntax Description**

| `url` | URL (accessible by the Cisco file system) used for saving archive files of the running configuration file in the Cisco configuration archive. |

**Command Default**

If this command is not configured, no location or filename prefix is specified for files in the Cisco configuration archive.

**Command Modes**

Archive configuration (config-archive)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>
Usage Guidelines

When this command is entered, an archive file of the running configuration is saved when the `archive config`, `write-memory`, or `copy running-config startup-config` command is entered.

URLs are commonly used to specify files or location on the World Wide Web. On Cisco devices, URLs can be used to specify the location of a file or directory on a device or a remote file server. The `path` command uses a URL to specify the location and filename prefix for the Cisco configuration archive.

The locations or file systems that you can specify in the `url` argument are as follows:

- If your platform has `disk0--disk0::`, `disk1::`, `ftp::`, `pram::`, `rcp::`, `slavedisk0::`, `slavedisk1::`, or `tftp`
- If your platform does not have `disk0--ftp::`, `http::`, `pram::`, `rcp::`, or `tftp`

The colon is required in the location format.

The filename of the first archive file is the filename specified in the `url` argument followed by `-1`. The filename of the second archive file is the filename specified in the `url` argument followed by `-2` and so on.

Because some file systems are incapable of storing the date and time that a file was written, the filename of the archive file can contain the date, time, and device hostname. To include the device hostname in the archive file filename, enter the characters `$h` (for example, `disk0:$h`). To include the date and time in the archive file filename, enter the characters `$t`.

When a configuration archive operation is attempted on a local file system, the file system is tested to determine if it is writable and if it has sufficient space to save an archive file. If the file system is read-only or if there is not enough space to save an archive file, an error message is displayed.

If you specify the `tftp::` file server as the location with the `path` command, you need to create the configuration file on the TFTP file server and change the file’s privileges before the `archive config` command works properly.

Examples

The following example of the `path` command shows how to specify the hostname, date, and time as the filename prefix for which to save archive files of the running configuration. In this example, the `time-period` command is also configured to automatically save an archive file of the running configuration every 20 minutes.

```
configure terminal
!
archive
  path disk0:$h$t
  time-period 20
end
```

The following is sample output from the `show archive` command illustrating the format of the resulting configuration archive filenames.

```
Device# show archive
There are currently 3 archive configurations saved.
The next archive file will be named routerJan-16-01:12:23.019-4
 Archive # Name
 0  
 1 disk0:routerJan-16-00:12:23.019-1
 2 disk0:routerJan-16-00:32:23.019-2
 3 disk0:routerJan-16-00:52:23.019-3 <- Most Recent
 4
 5
 6
 7
 8
```
### Cisco Configuration Archive on the TFTP File Server

The following example shows how to use the `path` command to specify the TFTP file server, address 10.48.71.226, as the archive configuration location and router-cfg as the configuration filename. First you create the configuration file on the TFTP server and change the file’s privileges, then you can save the configuration file to the configuration archive.

The following example shows the commands to use to create the file and change the file’s privileges on the TFTP server (UNIX commands):

```
> touch router-cfg-1
> chmod 777 router-cfg-1
```

The following example show how to create the configuration archive, save the running configuration to the archive, and display the files in the archive:

```
configure terminal
!
archive
    path tftp://10.48.71.226/router-cfg
exit
exit
!
archive config
Device# show archive
The next archive file will be named tftp://10.48.71.226/router-cfg-2
Archive # Name
  0
  1  tftp://10.48.71.226/router-cfg-1 <- Most Recent
  2
  3
  4
  5
  6
  7
  8
  9
 10
 11
 12
 13
 14
```

The following is sample output from the `show archive` command if you did not create the configuration file on the TFTP server before attempting to archive the current running configuration file:

```
configure terminal
!
archive
    path tftp://10.48.71.226/router-cfg
```
exit
exit
archive config
Device# show archive
The next archive file will be named tftp://10.48.71.226/router-cfg-1
Archive #   Name
  0
  1
  2
  3
  4
  5
  6
  7
  8
  9
 10
 11
 12
 13
 14

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Enters archive configuration mode.</td>
</tr>
<tr>
<td>archive config</td>
<td>Saves a copy of the current running configuration to the Cisco configuration archive.</td>
</tr>
<tr>
<td>configure confirm</td>
<td>Confirms replacement of the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td>configure replace</td>
<td>Replaces the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td>maximum</td>
<td>Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td>show archive</td>
<td>Displays information about the files saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td>time-period</td>
<td>Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.</td>
</tr>
</tbody>
</table>

**periodic**

To specify a recurring (weekly) time range for functions that support the time-range feature, use the periodic command in time-range configuration mode. To remove the time limitation, use the no form of this command.

```
periodic  days-of-the-week  hh:mm  to  [days-of-the-week]  hh:mm
no  periodic  days-of-the-week  hh:mm  to  [days-of-the-week]  hh:mm
```
Syntax Description

`days-of-the-week`  The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect.

This argument can be any single day or combinations of days: `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`, and `Sunday`. Other possible values are:

- **daily** --Monday through Sunday
- **weekdays** --Monday through Friday
- **weekend** --Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

`hh:mm`  The first occurrence of this argument is the starting hours:minutes that the associated time range is in effect. The second occurrence is the ending hours:minutes the associated statement is in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

`to`  Entry of the `to` keyword is required to complete the range “from start-time to end-time.”

Command Default

No recurring time range is defined.

Command Modes

Time-range configuration (config-time-range)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For Cisco IOS Release 12.2(11)T, IP and Internetwork Packet Exchange (IPX) extended access lists are the only functions that can use time ranges. For further information on using these functions, refer to the *Cisco IOS IP Configuration Guide* and the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*.

The `periodic` command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the `absolute` command. Use either of these commands after the `time-range` global configuration command, which specifies the name of the time range. Multiple `periodic` entries are allowed per `time-range` command.

If the end days-of-the-week value is the same as the start value, they can be omitted.

If a `time-range` command has both `absolute` and `periodic` values specified, then the `periodic` items are evaluated only after the `absolute start` time is reached, and are not further evaluated after the `absolute end` time is reached.

![Note](https://example.com/note_icon.png)

All time specifications are taken as local time. To ensure that the time range entries take effect at the desired times, you should synchronize the system software clock using Network Time Protocol (NTP).
The table below lists some typical settings for your convenience:

<table>
<thead>
<tr>
<th>If you want:</th>
<th>Configure this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday through Friday, 8:00 a.m. to 6:00 p.m. only</td>
<td>periodic weekday 8:00 to 18:00</td>
</tr>
<tr>
<td>Every day of the week, from 8:00 a.m. to 6:00 p.m. only</td>
<td>periodic daily 8:00 to 18:00</td>
</tr>
<tr>
<td>Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.</td>
<td>periodic monday 8:00 to 20:00</td>
</tr>
<tr>
<td>All weekend, from Saturday morning through Sunday night</td>
<td>periodic weekend 00:00 to 23:59</td>
</tr>
<tr>
<td>Saturdays and Sundays, from noon to midnight</td>
<td>periodic weekend 12:00 to 23:59</td>
</tr>
</tbody>
</table>

Examples

The following example configuration denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

Router# show startup-config

```
.time-range no-http
  periodic weekdays 8:00 to 18:00
!
.ip access-list extended strict
  deny tcp any any eq http time-range no-http
!
.interface ethernet 0
  ip access-group strict in
.
.
```

The following example configuration permits Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

Router# show startup-config

```
.time-range testing
  periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
  permit tcp any any eq telnet time-range testing
!
.interface ethernet 0
  ip access-group legal in
.
.
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>absolute</td>
<td>Specifies an absolute start and end time for a time range.</td>
</tr>
<tr>
<td>access-list (extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>deny (IP)</td>
<td>Sets conditions under which a packet does not pass a named IP access list.</td>
</tr>
<tr>
<td>permit (IP)</td>
<td>Sets conditions under which a packet passes a named IP access list.</td>
</tr>
<tr>
<td>time-range</td>
<td>Enables time-range configuration mode and names a time range definition.</td>
</tr>
</tbody>
</table>

### ping

To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the `ping` command in user EXEC or privileged EXEC mode.

```
ping [{{protocol  [tag]}}{host-namesystem-address}]`
```

#### Syntax Description

- **protocol** (Optional) Protocol keyword, either `appletalk`, `atm`, `clns`, `decdn`, `ip`, or `srb`. If a protocol is not specified, a basic ping will be sent using IP (IPv4). For extended options for ping over IP, see the documentation for the `ping ip` command.

  The `ping atm interface atm`, `ping ip`, `ping ipv6`, `ping sna`, and `ping vrf` commands are documented separately.

- **tag** (Optional) Specifies a tag encapsulated IP (tagIP) ping.

- **host-name** Hostname of the system to ping. If a `host-name` or `system-address` is not specified at the command line, it will be required in the `ping` system dialog.

- **system-address** Address of the system to ping. If a `host-name` or `system-address` is not specified at the command line, it will be required in the `ping` system dialog.

#### Command Default

This command has no default values.

#### Command Modes

User EXEC (>) Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>ping sna</code> command was introduced.</td>
</tr>
<tr>
<td>12.1(12c)E</td>
<td>The <code>ping vrf</code> command was introduced.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>Support for the IPv6 protocol was added.</td>
</tr>
</tbody>
</table>
The `ping` command sends an echo request packet to an address, then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning. For example, the `ping clns` command sends International Organization for Standardization (ISO) CLNS echo packets to test the reachability of a remote router over a connectionless Open System Interconnection (OSI) network.

If you enter the `ping` command without any keywords or argument values, an interactive system dialog prompts you for the additional syntax appropriate to the protocol you specify. (See the “Examples” section.)

To exit the interactive ping dialog before responding to all the prompts, type the escape sequence. The default escape sequence is Ctrl-^, X (Simultaneously press and release the Ctrl, Shift, and 6 keys and then press the X key). The escape sequence will vary depending on your line configuration. For example, another commonly used escape sequence is Ctrl-c.

The table below describes the test characters sent by the `ping` facility.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point indicates receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period indicates that the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error protocol data unit (PDU) was received.</td>
</tr>
<tr>
<td>C</td>
<td>A reply packet does not validate the reply data, and hence is marked &quot;Corrupted&quot;. Note This character will only appear if the &quot;validate&quot; option is selected in the ping request.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
</tbody>
</table>
A destination unreachable error protocol data unit (PDU) was received (Type 3) MTU required but DF bit set (code 4) with the “Next-Hop MTU” set to a non-zero value. If the “Next-hop MTU” is zero then ‘U’ is printed.

? Unknown packet type.

& Packet lifetime exceeded.

Note
Not all protocols require hosts to support pings. For some protocols, the pings are Cisco defined and can be answered only by another Cisco router.

The availability of protocol keywords depends on what protocols are enabled on your system.

Issuing the ping command in user EXEC mode will generally offer fewer syntax options than issuing the ping command in privileged EXEC mode.

Examples
After you enter the ping command in privileged EXEC mode, the system prompts you for a protocol keyword. The default protocol is IP.

If you enter a hostname or address on the same line as the ping command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the ping command using default values. The specific dialog varies somewhat from protocol to protocol.

Router# ping
Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms

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

### Table 36: ping Field Descriptions for IP

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target IP address:</td>
<td>Prompt for the IP address or hostname of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Repeat count [5]: | Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]: | Size of the ping packet (in bytes). Default: 100 bytes.
Extended commands [n]: | Specifies whether a series of additional commands appears.
Sweep range of sizes [n]: | Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.

!!!!!! | Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent | Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms | Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

The following example verifies connectivity to the neighboring ATM device for the ATM permanent virtual circuit (PVC) with the virtual path identifier (VPI)/virtual channel identifier (VCI) value 0/16:

```
Router# ping
Protocol [ip]: atm
ATM Interface: atm1/0
VPI value [0]:
VCI value [1]: 16
Loopback - End(0), Segment(1) [0]: 1
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The table below describes the default `ping` fields shown in the display.

### Table 37: `ping` Field Descriptions for ATM

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ATM Interface:</td>
<td>Prompt for the ATM interface.</td>
</tr>
<tr>
<td>VPI value [0]:</td>
<td>Prompt for the virtual path identifier. Default: 0.</td>
</tr>
<tr>
<td>VCI value [1]:</td>
<td>Prompt for the virtual channel identifier. Default: 1.</td>
</tr>
<tr>
<td>Loopback - End(0), Segment(1) [0]:</td>
<td>Prompt to specify end loopback, which verifies end-to-end PVC integrity, or segment loopback, which verifies PVC integrity to the neighboring ATM device. Default: segment loopback.</td>
</tr>
<tr>
<td>Repeat Count [5]:</td>
<td>Number of ping packets that will be sent to the destination address. Default: 5.</td>
</tr>
<tr>
<td>!!!!!!</td>
<td>Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.</td>
</tr>
<tr>
<td>Success rate is 100 percent</td>
<td>Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.</td>
</tr>
<tr>
<td>round-trip min/avg/max = 1/1/1 ms</td>
<td>Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping atm interface atm</td>
<td>Tests the connectivity of a specific PVC.</td>
</tr>
<tr>
<td>ping ip</td>
<td>Tests network connectivity on IP networks.</td>
</tr>
<tr>
<td>ping ipv6</td>
<td>Tests the connection to a remote host on the network using IPv6.</td>
</tr>
<tr>
<td>ping sna</td>
<td>Tests network integrity and timing characteristics over an SNA Switching network.</td>
</tr>
<tr>
<td>ping vrf</td>
<td>Tests the connection in the context of a specific VPN (VRF).</td>
</tr>
</tbody>
</table>

### ping (privileged)

To diagnose basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, VINES, or XNS networks, use the `ping` command in privileged EXEC command mode.

```
```
### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname</code></td>
<td>(Optional) Hostname of the system to ping.</td>
</tr>
<tr>
<td><code>system-address</code></td>
<td>(Optional) Address of the system to ping.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>(Optional) Protocol to use for the ping. Valid values are: <code>apollo</code>, <code>appletalk</code>, <code>clns</code>, <code>decnet</code>, <code>ethernet</code>, <code>ip</code>, <code>ipv6</code>, <code>ipx</code>, <code>srb</code>, <code>vines</code>, <code>xns</code>.</td>
</tr>
<tr>
<td><code>tag</code></td>
<td>(Optional) Specifies a tag encapsulated IP ping.</td>
</tr>
<tr>
<td><code>data</code></td>
<td>(Optional) Specifies the data pattern.</td>
</tr>
<tr>
<td><code>hex-data-pattern</code></td>
<td>(Optional) Hexadecimal value of the data in the range of 0 to FFFF.</td>
</tr>
<tr>
<td><code>df-bit</code></td>
<td>(Optional) Enables the “do not fragment” bit in the IP header.</td>
</tr>
<tr>
<td><code>repeat</code></td>
<td>(Optional) Specifies the number of times the ping should be sent.</td>
</tr>
<tr>
<td><code>repeat-count</code></td>
<td>(Optional) Integer in the range of 1 to 2147483647. The default is 5.</td>
</tr>
<tr>
<td><code>size</code></td>
<td>(Optional) Size, in bytes, of the ping datagram.</td>
</tr>
<tr>
<td><code>datagram-size</code></td>
<td>(Optional) Integer in the range of 40 to 18024.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>(Optional) Device sending the ping</td>
</tr>
<tr>
<td><code>source-address</code></td>
<td>(Optional) Address or name of the device sending the ping.</td>
</tr>
<tr>
<td><code>async</code></td>
<td>(Optional) Asynchronous interface.</td>
</tr>
<tr>
<td><code>bvi</code></td>
<td>(Optional) Bridge-Group Virtual interface.</td>
</tr>
<tr>
<td><code>ctunnel</code></td>
<td>(Optional) CTunnel interface.</td>
</tr>
<tr>
<td><code>dialer</code></td>
<td>(Optional) Dialer interface.</td>
</tr>
<tr>
<td><code>ethernet</code></td>
<td>(Optional) Ethernet IEEE 802.3 interface.</td>
</tr>
<tr>
<td><code>fastethernet</code></td>
<td>(Optional) FastEthernet IEEE 802.3 interface.</td>
</tr>
<tr>
<td><code>lex</code></td>
<td>(Optional) Lex interface.</td>
</tr>
<tr>
<td><code>loopback</code></td>
<td>(Optional) Loopback interface.</td>
</tr>
<tr>
<td><code>multilink</code></td>
<td>(Optional) Multilink-group interface.</td>
</tr>
<tr>
<td><code>null</code></td>
<td>(Optional) Null interface.</td>
</tr>
<tr>
<td><code>port-channel</code></td>
<td>(Optional) Ethernet channel of interfaces.</td>
</tr>
<tr>
<td><code>tunnel</code></td>
<td>(Optional) Tunnel interface</td>
</tr>
<tr>
<td><code>vif</code></td>
<td>(Optional) Pragmatic General Multicast (PGM) host interface</td>
</tr>
<tr>
<td><code>virtual-template</code></td>
<td>(Optional) Virtual Template interface.</td>
</tr>
<tr>
<td><code>virtual-tokenring</code></td>
<td>(Optional) Virtual TokenRing.</td>
</tr>
</tbody>
</table>
**Command Default**

A ping operation is not performed.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The following keywords were added in Cisco IOS Release 12.0: <strong>data</strong>, <strong>df-bit</strong>, <strong>repeat</strong>, <strong>size</strong>, <strong>source</strong>, <strong>timeout</strong>, <strong>validate</strong>.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>The ethernet option for protocol was added in Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ping** (packet internet groper) command tests the reachability of a remote router over a connectionless Open System Interconnection (OSI) network. The command sends ISO CLNS echo packets to an address and waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

When you type the **ping** command, you are prompted to enter options before the **ping** command executes. The characters in brackets ([ ]) indicate default values. When you want to use a default value, press Enter on your keyboard.

If you enter a hostname or system address when you enter the **ping** command, the default action is taken for the protocol type of that hostname or system address.

The optional **data**, **df-bit**, **repeat**, **size**, **source**, **timeout**, and **validate** keywords can be used to prevent extended **ping** command output. You can use as many of these keywords as you need, and you can use them in any order after the **hostname** or **system-address** arguments.

When you enter the **ethernet** protocol option, you will be prompted to enter MAC address and maintenance domain in addition to the information common across protocols.

To terminate a ping session before it completes, type the escape sequence (Ctrl-^X) by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys and then pressing the X key.

**Note**

Not all protocols require hosts to support pings. For some protocols, the pings are defined by Cisco and answered only by a Cisco router.

The table below describes the test characters that the ping operation uses.
Table 38: ping Command Response Characters and Their Meanings

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>Destination unreachable error protocol data unit (PDU) was received.</td>
</tr>
<tr>
<td>C</td>
<td>A reply packet does not validate the reply data, and hence is marked &quot;Corrupted&quot;. Note: This character will only appear if the &quot;validate&quot; option is selected in the ping request.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

Examples

The following example shows a ping command and output. The precise dialog varies from protocol to protocol, but all are similar to the ping session shown here using default values.

Router# ping
Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms

The following example shows how to send a ping specifying the ethernet protocol option, MAC address, and maintenance domain and using the default values for the remaining parameters:

Router# ping
Protocol [ip]: ethernet
Mac Address: aabb.cc00.0410
Maintenance Domain: DOMAIN_PROVIDER_L5_1 VLAN [0]: 2 Source MPID [1522]:
Repeat Count [5]:
Datagram Size [107]:
Timeout in seconds [2]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/8 ms.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping ethernet</td>
<td>Sends Ethernet CFM loopback messages to a destination MAC address.</td>
</tr>
<tr>
<td>ping (user)</td>
<td>Tests the connection to a remote host on the network.</td>
</tr>
<tr>
<td>ping vrf</td>
<td>Tests the connection to a remote device in a VPN.</td>
</tr>
</tbody>
</table>

**ping ip**

To test network connectivity on IP networks, use the **ping ip** command in privileged EXEC mode.

```
ping ip {host-name|ip-address} [{data [hex-data-pattern]|df-bit}|repeat [repeat-count]|tos [service value]|size [datagram-size] source {source-address|source-interface}] [timeout seconds] [validate] [verbose]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-name</td>
<td>Host name of the system to ping.</td>
</tr>
<tr>
<td>system-address</td>
<td>Address of the system to ping.</td>
</tr>
<tr>
<td>data</td>
<td>(Optional) Specifies the data pattern. Range is from 0 to FFFF.</td>
</tr>
<tr>
<td>df-bit</td>
<td>(Optional) Enables the “do-not-fragment” bit in the IP header.</td>
</tr>
<tr>
<td>repeat</td>
<td>(Optional) Specifies the number of pings sent. The range is from 1 to 2147483647. The default is 5.</td>
</tr>
<tr>
<td>tos</td>
<td>(Optional) Specifies the type of service value. The range is from 1 to 255.</td>
</tr>
<tr>
<td>size</td>
<td>(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.</td>
</tr>
<tr>
<td>datagram-size</td>
<td>(Optional) Range is from 40 to 18024.</td>
</tr>
<tr>
<td>source</td>
<td>(Optional) Specifies the source address or source interface.</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional) IP address to use as the source in the ping packets.</td>
</tr>
</tbody>
</table>
The availability of these keywords depends on your system hardware.

(Optional) Name of the interface from which the ping should be sent, and the Interface ID (slot/port/number). Interface name keywords include the following:

• async (Asynchronous Interface)
• bvi (Bridge-Group Virtual Interface)
• ctunnel
• dialer
• ethernet
• fastEthernet
• lex
• loopback
• multilink (Multilink-group interface)
• null
• port-channel (Ethernet channel of interfaces)
• tunnel
• vif (PGM Multicast Host interface)
• virtual-template
• virtual-tokenring
• xtagatm (Extended Tag ATM interface)

(Optional) Specifies the timeout interval in seconds. The default is 2 seconds. Range is from 0 to 3600.

(Optional) Validates the reply data.

(Optional) Enables verbose output, which lists individual ICMP packets, as well as Echo Responses.

Command Modes

Privileged Exec

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The data, df-bit, repeat, size, source, timeout, and validate keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.2(02)S</td>
<td>The tos keyword was added.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

To abnormally terminate a ping session, type the escape sequence--by default, *Ctrl-^ X*. You type the default by simultaneously pressing and releasing the *Ctrl*, *Shift*, and *6* keys, and then pressing the *X* key.

The table below describes the test characters that the ping facility sends.

### Table 39: ping Test Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point indicates receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period indicates that the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error protocol data unit (PDU) was received.</td>
</tr>
<tr>
<td>C</td>
<td>A reply packet does not validate the reply data, and hence is marked &quot;Corrupted&quot;. <em>Note</em> This character will only appear if the &quot;validate&quot; option is selected in the ping request.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

*Note* Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

Examples

After you enter the **ping** command in privileged mode, the system prompts you for a protocol keyword. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The optional **data**, **df-bit**, **repeat**, **size**, **source**, **timeout**, and **validate** keywords can be used to avoid extended **ping** command output. You can use as many of these keywords as you need, and you can use them in any order after the **host-name** or **system-address** arguments.

Although the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session using default values shown in the following output:

```
Router# ping
Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms

The table below describes the default ping fields shown in the display.

### Table 40: ping Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol [ip]:</td>
<td>Prompts for a supported protocol. The default is IP.</td>
</tr>
<tr>
<td>Target IP address:</td>
<td>Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. The default is none.</td>
</tr>
<tr>
<td>Repeat count [5]:</td>
<td>Prompts for the number of ping packets that will be sent to the destination address. The default is 5 packets.</td>
</tr>
<tr>
<td>Datagram size [100]:</td>
<td>Prompts for the size of the ping packet (in bytes). The default is 100 bytes.</td>
</tr>
<tr>
<td>Timeout in seconds [2]:</td>
<td>Prompts for the timeout interval. The default is 2 seconds.</td>
</tr>
<tr>
<td>Extended commands [n]:</td>
<td>Specifies whether a series of additional commands appears.</td>
</tr>
<tr>
<td>Sweep range of sizes [n]:</td>
<td>Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.</td>
</tr>
<tr>
<td>!!!!!!</td>
<td>Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.</td>
</tr>
<tr>
<td>Success rate is 100 percent</td>
<td>Indicates the percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.</td>
</tr>
<tr>
<td>round-trip min/avg/max = 1/2/4 ms</td>
<td>Indicates the round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping ipv6</td>
<td>Tests the connection to a remote host on the network using IPv6.</td>
</tr>
<tr>
<td>ping vrf</td>
<td>Tests the connection in the context of a specific VPN (VRF).</td>
</tr>
</tbody>
</table>

### ping srb

To test network connectivity for Source Route Bridging (SRB) networks, use the ping srb command in privileged EXEC mode.

ping srb name
Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping vrf</td>
<td>Tests network connectivity on IP networks.</td>
</tr>
</tbody>
</table>

Command Modes

- Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to ping the target host of IP address 192.0.2.1:

```
Router# ping srb 192.0.2.1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>Tests network connectivity on IP networks.</td>
</tr>
<tr>
<td>ping vrf</td>
<td>Tests network connectivity on IP networks.</td>
</tr>
</tbody>
</table>

ping vrf

To test a connection in the context of a specific VPN connection, use the `ping vrf` command in user EXEC or privileged EXEC mode.

```
ping vrf vrf-name [tag] [connection] target-address [connection-options]
```

Syntax Description

- `vrf-name`: The name of the VPN (VRF context).
- `tag`: (Optional) Specifies a tag encapsulated IP (tagIP) ping.
- `connection`: (Optional) Connection options include `atm`, `clns`, `decnet`, `ip`, `ipv6`, `ipx`, `sna`, or `srb`. The default is `ip`.
- `target-address`: The destination ID for the ping operation. Usually, this is the IPv4 address of the host. For example, the target for an IPv4 ping in a VRF context would be the IPv4 address or domain name of the target host. The target for an IPv6 ping in a VRF context would be the IPv6 prefix or domain name of the target host.
  - If the target address is not specified, the CLI will enter the interactive dialog for ping.
connection-options (Optional) Each connection type may have its own set of connection options. For example, connection options for IPv4 are source, df-bit, and timeout. See the appropriate ping command documentation for details.

Command Default

The default connection type for ping is IPv4.

Command Modes

User EXEC

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(12c)E, 12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>12.2(33)SCF</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SCF.</td>
</tr>
</tbody>
</table>

Usage Guidelines

A VPN routing and forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the ping vrf command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard ping command will not usually work. The ping vrf command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the “Examples” section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the “CustomerA” VPN connection.

Router# ping vrf CustomerA 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the “ip” protocol is specified, but no address is given:

Router# ping vrf CustomerB ip
Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Cisco IOS Configuration Fundamentals Command Reference
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern (0xABCD):
Loose, Strict, Record, Timestamp, Verbose[none]: Record

Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options: Total option bytes= 39, padded length=40
Record route: <*>
  (0.0.0.0)
  (0.0.0.0)
  (0.0.0.0)
  (0.0.0.0)
  (0.0.0.0)
  (0.0.0.0)
  (0.0.0.0)
  (0.0.0.0)
.
.
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

The following examples shows the various options for IP in the ping vrf command:

Router# show parser dump exec | include ping vrf

1 ping vrf <string>
1 ping vrf <string> ip <string>
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb

Cisco CMDS Routers: Example

The following example shows how to verify the matching and marking configuration in an MPLS network:
Router# ping vrf vrfa 1.3.99.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.3.99.98, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/20 ms

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping atm interface atm</td>
<td>Tests the connectivity of a specific PVC.</td>
</tr>
<tr>
<td>ping ip</td>
<td>Tests the connection to a remote host on the network using IPv4.</td>
</tr>
<tr>
<td>ping ipv6</td>
<td>Tests the connection to a remote host on the network using IPv6.</td>
</tr>
<tr>
<td>ping sna</td>
<td>Tests network integrity and timing characteristics over an SNA Switching network.</td>
</tr>
</tbody>
</table>

### platform shell

To grant shell access and enter shell access grant configuration mode, use the **platform shell** command in global configuration mode. To disable this function, use the **no** form of this command.

```
platform shell
no platform shell
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command has no arguments or keywords.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command is disabled.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration (config)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>12.2(33)XNC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command should be entered before using the request platform software system shell command.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to grant shell access:

```
Router(config)# platform shell
Router(config)#
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request platform software system shell</td>
<td>Requests platform shell access.</td>
</tr>
</tbody>
</table>
power enable

To turn on power for the modules, use the `power enable` command in global configuration mode. To power down a module, use the `no` form of this command.

```
power enable module slot
no power enable module slot
```

**Syntax Description**

<table>
<thead>
<tr>
<th>module</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a module slot number; see the “Usage Guidelines” section for valid values.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

Enabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was changed to allow you to disable power to empty slots.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enter the `no power enable module slot` command to power down a module, the module’s configuration is not saved.

When you enter the `no power enable module slot` command to power down an empty slot, the configuration is saved.

The `slot` argument designates the module number. Valid values for `slot` depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

**Examples**

This example shows how to turn on the power for a module that was previously powered down:

```
Router(config) #
power enable module 5
Router(config) #
```

This example shows how to power down a module:

```
Router(config) #
no power enable module 5
Router(config) #
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show power</td>
<td>Displays information about the power status.</td>
</tr>
</tbody>
</table>
power redundancy-mode

To set the power-supply redundancy mode, use the `power redundancy-mode` command in global configuration mode.

```
power redundancy-mode {combined|redundant}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Estimate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>combined</code></td>
<td>Specifies no redundancy (combine power-supply outputs).</td>
</tr>
<tr>
<td><code>redundant</code></td>
<td>Specifies redundancy (either power supply can operate the system).</td>
</tr>
</tbody>
</table>

### Command Default

**redundant**

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to set the power supplies to the no-redundancy mode:

```
Router(config)#
power redundancy-mode combined
Router(config)#
```

This example shows how to set the power supplies to the redundancy mode:

```
Router(config)#
power redundancy-mode redundant
Router(config)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show power</code></td>
<td>Displays information about the power status.</td>
</tr>
</tbody>
</table>

printer

To configure a printer and assign a server tty line (or lines) to it, use the `printer` command in global configuration mode. To disable printing on a tty line, use the `no` form of this command.

```
printer printer-name [line number | rotary number] [formfeed] [j oobtimeout seconds] [newline-convert] [jobtypes type]
no printer printer-name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Estimate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>printer-name</code></td>
<td>Printer name.</td>
</tr>
</tbody>
</table>
line  number  Assigns a tty line to the printer.  
The number argument can be any one of the following parameters:  
  • aux  -- Specifies the auxiliary line.  
  • console  -- Specifies the primary terminal line.  
  • slot  / port  -- First slot and port numbers for the internal modems.  
  • tty  number  -- Specifies the terminal controller value.  
  • tty-number  -- tty number, in the range 0 to 491.  
  • vty  value  -- Specifies the virtual terminal value.  

rotary  number  Assigns a rotary group of tty lines to the printer.  

formfeed  (Optional) Causes the Cisco IOS software to send a form-feed character (ASCII 0x0C) to the printer tty line immediately following each print job received from the network.  

jobtimeout  seconds  (Optional) Changes the default time for line acquisition. The range is from 1 to 3600 seconds.  

newline-convert  (Optional) Converts newline (linefeed) characters to a two-character sequence “carriage-return, linefeed” (CR+LF).  

jobtypes  type  (Optional) Specifies allowed job types.  

<table>
<thead>
<tr>
<th>Command Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No printers are defined.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration (config)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>10.3</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
</tr>
<tr>
<td>15.0(1)M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command enables you to configure a printer for operations and assign either a single tty line or a group of tty lines to it. To make multiple printers available through the same printer name, specify the number of a rotary group.</td>
</tr>
<tr>
<td>In addition to configuring the printer with the printer command, you must modify the file /etc/printcap on your UNIX system to include the definition of the remote printer in the Cisco IOS software. Refer to the Cisco IOS Configuration Fundamentals Configuration Guide for additional information.</td>
</tr>
<tr>
<td>Use the optional newline-convert keyword in UNIX environments that cannot handle single-character line terminators. This converts newline characters to a carriage-return, linefeed sequence. Use the formfeed keyword when using the line printer daemon (lpd) protocol to print and your system is unable to separate</td>
</tr>
</tbody>
</table>
individual output jobs with a form feed (page eject). You can enter the `newline-convert` and `formfeed` keywords together and in any order.

**Examples**

The following example shows how to configure a printer named printer1 and to assign the output to tty line 4:

```
Router# configure terminal
Router(config)# printer printer1 line 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear line</code></td>
<td>Returns a terminal line to idle state.</td>
</tr>
</tbody>
</table>

**private**

To save user EXEC command changes between terminal sessions, use the `private` command in line configuration mode. To restore the default condition, use the `no` form of this command.

```
private
no private
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

User-set configuration options are cleared with the `exit` EXEC command or when the interval set with the `exec-timeout` line configuration command has passed.

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command ensures that the terminal parameters set by the user remain in effect between terminal sessions. This behavior is desirable for terminals in private offices.

**Examples**

In the following example, line 15 (in this example, vty 1) is configured to keep all user-supplied settings at system restarts:

```
Router(config)# line 15
Router(config-line)# private
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exec-timeout</code></td>
<td>Sets the interval that the EXEC command interpreter waits until user input is detected.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits any configuration mode, or closes an active terminal session and terminates the EXEC.</td>
</tr>
</tbody>
</table>
process cpu statistics limit entry-percentage

To set the process entry limit and the size of the history table for CPU utilization statistics, use the `process cpu statistics limit entry-percentage` command in global configuration mode. To disable CPU utilization statistics, use the `no` form of this command.

```
process cpu statistics limit entry-percentage number [size seconds]
no process cpu statistics limit entry-percentage
```

**Syntax Description**

| **number** | Integer from 1 to 100 that indicates the percentage of CPU utilization that a process must use to become part of the history table. |
| **size seconds** | (Optional) Changes the duration of time in seconds for which CPU statistics are stored in the history table. Valid values are 5 to 86400. The default is 600. |

**Command Default**

`size seconds`: 600 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `process cpu statistics limit entry-percentage` command to set the entry limit and size of CPU utilization statistics.

**Examples**

The following example shows how to set an entry limit at 40 percent and a size of 300 seconds:

```
configure terminal
!
process cpu statistics limit entry-percentage 40 size 300
end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>process cpu threshold type</code></td>
<td>Defines CPU usage thresholds that, when crossed, cause a CPU threshold notification.</td>
</tr>
<tr>
<td><code>snmp-server enable traps cpu</code></td>
<td>Enables CPU threshold violations traps.</td>
</tr>
<tr>
<td><code>snmp-server host</code></td>
<td>Specifies the recipient of SNMP notifications.</td>
</tr>
</tbody>
</table>
process cpu threshold type

To set CPU thresholding notification types and values, use the `process cpu threshold type` command in global configuration mode. To disable CPU thresholding notifications, use the `no` form of this command.

```
process cpu threshold type {total|process|interrupt} rising percentage interval seconds [falling fall-percentage interval seconds]
no process cpu threshold type {total|process|interrupt}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>total</code></td>
<td>Sets the CPU threshold type to total CPU utilization.</td>
</tr>
<tr>
<td><code>process</code></td>
<td>Sets the CPU threshold type to CPU process utilization.</td>
</tr>
<tr>
<td><code>interrupt</code></td>
<td>Sets the CPU threshold type to CPU interrupt utilization.</td>
</tr>
<tr>
<td><code>rising percentage</code></td>
<td>The percentage (1 to 100) of CPU resources that, when exceeded for the configured interval, triggers a CPU thresholding notification.</td>
</tr>
<tr>
<td><code>interval seconds</code></td>
<td>The duration of the CPU threshold violation, in seconds (5 to 86400), that must be met to trigger a CPU thresholding notification.</td>
</tr>
<tr>
<td><code>falling fall-percentage</code></td>
<td>(Optional) The percentage (1 to 100) of CPU resources that, when usage falls below this level for the configured interval, triggers a CPU thresholding notification.</td>
</tr>
<tr>
<td>- This value must be equal to or less than the <code>rising percentage</code> value.</td>
<td></td>
</tr>
<tr>
<td>- If not specified, the <code>falling fall-percentage</code> value is set to the same value as the <code>rising percentage</code> value.</td>
<td></td>
</tr>
</tbody>
</table>

### Command Default

CPU thresholding notifications are disabled.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command defines CPU usage thresholds that, when crossed, cause a CPU thresholding notification. When this command is enabled, Cisco IOS software polls the system at the configured interval. Notification occurs in two situations:

- When a configured CPU usage threshold is exceeded (`rising percentage`)
- When CPU usage falls below the configured threshold (`falling fall-percentage`)
Examples

The following example shows how to set the total CPU utilization notification threshold at 80 percent for a rising threshold notification and 20 percent for a falling threshold notification, with a 5-second polling interval:

```plaintext
configure terminal
!
process cpu threshold type total rising 80 interval 5 falling 20 interval 5
end
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process cpu statistics limit entry</td>
<td>Sets the entry limit and size of CPU utilization statistics.</td>
</tr>
<tr>
<td>snmp-server enable traps cpu</td>
<td>Enables CPU threshold violations traps.</td>
</tr>
<tr>
<td>snmp-server host</td>
<td>Specifies the recipient of SNMP notifications.</td>
</tr>
</tbody>
</table>

**process-max-time**

To configure the amount of time after which a process should voluntarily yield to another process, use the `process-max-time` command in global configuration mode. To reset this value to the system default, use the `no` form of this command.

```plaintext
process-max-time milliseconds
no process-max-time milliseconds
```

**Syntax Description**

| `milliseconds` | Maximum duration (in milliseconds) that a process can run before suspension. The range is from 20 to 200 milliseconds. |

**Command Default**

The default maximum process time is 200 milliseconds.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Lowering the maximum time a process can run is useful in some circumstances to ensure equitable division of CPU time among different tasks.

Only use this command if recommended to do so by the Cisco Technical Assistance Center (TAC).

**Examples**

The following example limits the duration that a process will run to 100 milliseconds:

```plaintext
Router(config)# process-max-time 100
```
prompt

To customize the CLI prompt, use the `prompt` command in global configuration mode. To revert to the default prompt, use the `no` form of this command.

```
prompt string
no prompt [string]
```

**Syntax Description**

| string | Text that will be displayed on screen as the CLI prompt, including any desired prompt variables. |

**Command Default**

The default prompt is either `Router` or the name defined with the `hostname` global configuration command, followed by an angle bracket (`>` for user EXEC mode or a pound sign (`#`) for privileged EXEC mode.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can include customized variables when specifying the prompt. All prompt variables are preceded by a percent sign (`%`). The table below lists the available prompt variables.

<table>
<thead>
<tr>
<th>Prompt Variable</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%h</code></td>
<td>Host name. This is either <code>Router</code> or the name defined with the <code>hostname</code> global configuration command.</td>
</tr>
<tr>
<td><code>%n</code></td>
<td>Physical terminal line (tty) number of the EXEC user.</td>
</tr>
<tr>
<td><code>%p</code></td>
<td>Prompt character itself. It is either an angle bracket (<code>&gt;</code> for user EXEC mode or a pound sign (<code>#</code>) for privileged EXEC mode.</td>
</tr>
<tr>
<td><code>%s</code></td>
<td>Space.</td>
</tr>
<tr>
<td><code>%t</code></td>
<td>Tab.</td>
</tr>
<tr>
<td><code>%%</code></td>
<td>Percent sign (%)</td>
</tr>
</tbody>
</table>

Issuing the `prompt %h` command has the same effect as issuing the `no prompt` command.

**Examples**

The following example changes the EXEC prompt to include the tty number, followed by the name and a space:

```
Router(config)# prompt TTY%n@%h%s%p
```

The following are examples of user and privileged EXEC prompts that result from the previous command:
TTY17@Router1 > enable
TTY17@Router1 #

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname</code></td>
<td>Specifies or modifies the host name for the network server.</td>
</tr>
</tbody>
</table>

### prompt config

To configure the system’s prompt for configuration mode, use the `prompt config` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
prompt config hostname-length number
no prompt [config]
```

#### Syntax Description

| `hostname-length` | Sets the length of the hostname in the configuration prompt.            |
| `number`          | Maximum length of the hostname. The range is from 0 to 80.             |

#### Command Default

The system's prompt is not configured for configuration mode.

#### Command Modes

Global configuration (config)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

#### Examples

This example shows how to configure the system’s prompt for configuration mode:

```
Router(config)#
prompt config hostname-length 4
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>prompt</code></td>
<td>Customizes the CLI prompt.</td>
</tr>
</tbody>
</table>

### pwd

To show the current setting of the `cd` command, use the `pwd` command in EXEC mode.

```
pwd
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Modes

User EXEC
Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `pwd` command to show which directory or file system is specified as the default by the `cd` command. For all EXEC commands that have an optional `filesystem` argument, the system uses the file system specified by the `cd` command when you omit the optional `filesystem` argument.

For example, the `dir` command contains an optional `filesystem` argument and displays a list of files on a particular file system. When you omit this `filesystem` argument, the system shows a list of the files on the file system specified by the `cd` command.

### Examples

The following example shows that the present working file system specified by the `cd` command is slot 0:

```
Router> pwd
slot0: /
```

The following example uses the `cd` command to change the present file system to slot 1 and then uses the `pwd` command to display that present working file system:

```
Router> cd slot1:
Router> pwd
slot1: /
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
</tbody>
</table>
R through setup

- R through setup, on page 400
refuse-message

To define and enable a line-in-use message, use the refuse-message command in line configuration mode. To disable the message, use the no form of this command.

refuse-message  d  message  d
no  refuse-message

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>Delimiting character of your choice--a pound sign (#), for example. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td>message</td>
<td>Message text.</td>
</tr>
</tbody>
</table>

Command Default

Disabled (no line-in-use message is displayed).

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. You cannot use the delimiting character within the text of the message.

When you define a message using this command, the Cisco IOS software performs the following steps:

1. Accepts the connection.
2. Prints the custom message.
3. Clears the connection.

Examples

In the following example, line 5 is configured with a line-in-use message, and the user is instructed to try again later:

    line 5
    refuse-message  /The dial-out modem is currently in use. Please try again later./
regexp optimize

To optimize the compilation of a regular expression access list, use the `regexp optimize` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
regexp optimize
no regexp optimize
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The command is enabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td></td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to optimize the compilation of regular expression access list:

```
Router# configure terminal
Router(config)# regexp optimize
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>regexp (profile map configuration)</code></td>
<td>Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.</td>
</tr>
</tbody>
</table>

**reload**

To reload the operating system, use the `reload` command in privileged EXEC or diagnostic mode.

```
reload [{/verify[/noverify]} [{/warm file} [{/line in {hhh:mm|mmmm [text]}]}]at hh:mm [day month] [text]]] [reason [reason-string]|cancel]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/verify</code></td>
<td>(Optional) Verifies the digital signature of the file that will be loaded onto the operating system.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#) Diagnostic (diag)</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was modified. Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>This command was modified. The warm keyword was added.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S. The /verify and /noverify keywords were added.</td>
</tr>
<tr>
<td>12.2(20)S</td>
<td>This command was modified. Support was added for the Cisco 7304 router. The Cisco 7500 series router in not supported in Cisco IOS Release 12.2(20)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was modified. The /verify and /noverify keywords were integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>/noverify</th>
<th>(Optional) Does not verify the digital signature of the file that will be loaded onto the operating system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>This keyword is often issued if the file verify auto command is enabled, which automatically verifies the digital signature of all images that are copied.</td>
</tr>
<tr>
<td>warm</td>
<td>(Optional) Specifies warm rebooting.</td>
</tr>
<tr>
<td>file</td>
<td>(Optional) Specifies the image file for warm rebooting.</td>
</tr>
<tr>
<td>line</td>
<td>(Optional) Reason for relogging; the string can be from 1 to 255 characters long.</td>
</tr>
<tr>
<td>in hhh : mm</td>
<td>(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.</td>
</tr>
<tr>
<td>text</td>
<td>(Optional) Reason for relogging; the string can be from 1 to 255 characters long.</td>
</tr>
<tr>
<td>at hh : mm</td>
<td>(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.</td>
</tr>
<tr>
<td>day</td>
<td>(Optional) Number of the day in the range from 1 to 31.</td>
</tr>
<tr>
<td>month</td>
<td>Month of the year.</td>
</tr>
<tr>
<td>reason reason-string</td>
<td>(Optional) Specifies a reason for relogging.</td>
</tr>
<tr>
<td>cancel</td>
<td>(Optional) Cancels a scheduled reload.</td>
</tr>
</tbody>
</table>
This command was modified. The `/verify` and `/noverify` keywords were integrated into Cisco IOS Release 12.3(4)T.

This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

This command was modified. The `file` keyword and `url` argument were added.

This command was integrated into Cisco IOS Release 12.2(28)SB.

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

This command was modified. The `reason` keyword and `reason-string` argument were added.

This command was introduced on the Cisco ASR 1000 Series Aggregation Services Router and was made available in diagnostic mode.

### Usage Guidelines

The `reload` command halts the system. If the system is set to restart on error, it reboots itself. Use the `reload` command after configuration information is entered into a file and saved to the startup configuration.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This restriction prevents the system from using an image stored in the ROM monitor and taking the system out of the remote user’s control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system prompts whether you want to proceed with the save if the CONFIG_FILE variable points to a startup configuration file that no longer exists. If you respond “yes” in this situation, the system enters setup mode upon reload.

When you schedule a reload to occur at a later time (using the `in` keyword), it must take place within 24 days.

The `at` keyword can be used only if the system clock has been set on the router (either through Network Time Protocol [NTP], the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, synchronize the time on each router with NTP.

When you specify the reload time using the `at` keyword, if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

To display information about a scheduled reload, use the `show reload` command.

### The `/verify` and `/noverify` Keywords

If the `/verify` keyword is specified, the integrity of the image will be verified before it is reloaded onto a router. If verification fails, the image reload will not occur. Image verification is important because it assures the user that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

The `/noverify` keyword overrides any global automatic image verification that may be enabled via the `file verify auto` command.
The warm Keyword

If you issue the `reload` command after you have configured the `warm-reboot` global configuration command, a cold reboot will occur. Thus, if you want to reload your system, but do not want to override the warm reboot functionality, you should specify the `warm` keyword with the `reload` command. The warm reboot functionality allows a Cisco IOS image to reload without ROM monitor intervention. That is, read-write data is saved in RAM during a cold startup and restored during a warm reboot. Warm rebooting allows the router to reboot quicker than conventional rebooting (where control is transferred to ROM monitor and back to the image) because nothing is copied from flash to RAM.

Examples

The following example shows how to immediately reload the software on the router:

```
Router# reload
```

The following example shows how to reload the software on the router in 10 minutes:

```
Router# reload in 10
Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload? [confirm]
```

The following example shows how to reload the software on the router at 1:00 p.m. on that day:

```
Router# reload at 13:00
Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
```

The following example shows how to reload the software on the router on April 21 at 2:00 a.m.:

```
Router# reload at 02:00 apr 21
Router# Reload scheduled for 02:00:00 PDT Sat Apr 21 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
```

The following example shows how to cancel a pending reload:

```
Router# reload cancel
%Reload cancelled.
```

The following example shows how to perform a warm reboot at 4:00 a.m. on that day:

```
Router# reload warm at 04:00
```

The following example shows how to specify a reason for the reload:

```
Router# reload reason reloaded with updated version
```

The following example shows how to specify image verification via the `/verify` keyword before reloading an image onto the router:

```
Router# reload /verify
Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
............................................................Done!
```

```
<table>
<thead>
<tr>
<th>Embedded Hash</th>
<th>MD5: CFA258948C4ECE52085DCF428A426DCD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computed Hash</td>
<td>MD5: CFA258948C4ECE52085DCF428A426DCD</td>
</tr>
<tr>
<td>CCO Hash</td>
<td>MD5: 44A7B9BDDD9638128C35528466318183</td>
</tr>
</tbody>
</table>
```
remote command

To execute a Cisco 7600 series router command directly on the switch console or a specified module without having to log into the Cisco 7600 series router first, use the remote command command in privileged EXEC mode.

remote command {module num|standby-rp|switch} command

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module num</td>
<td>Specifies the module to access; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>standby-rp</td>
<td>Specifies the standby route processor.</td>
</tr>
<tr>
<td>switch</td>
<td>Specifies the active switch processor.</td>
</tr>
<tr>
<td>command</td>
<td>Command to be executed.</td>
</tr>
</tbody>
</table>

| Command Default | This command has no default settings. |

| Command Modes | Privileged EXEC |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>The standby-rp keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

| Usage Guidelines | The module num keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The module num keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only. When you execute the remote command switch command, the prompt changes to Switch-sp#. This command is supported on DFC-equipped modules and the supervisor engine only. |
This command does not support command completion, but you can use shortened forms of the command (for example, entering `sh` for `show`).

**Examples**

This example shows how to execute the `show calendar` command from the standby route processor:

```
Router# remote command standby-rp show calendar
Switch-sp# 09:52:50 UTC Mon Nov 12 2001
Router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote login</td>
<td>Accesses the Cisco 7600 series router console or a specific module.</td>
</tr>
</tbody>
</table>

**remote login**

To access the Cisco 7600 series router console or a specific module, use the `remote login` command in privileged EXEC mode.

```
remote login {module num|standby-rp|switch}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module num</td>
<td>Specifies the module to access; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>standby-rp</td>
<td>Specifies the standby route processor.</td>
</tr>
<tr>
<td>switch</td>
<td>Specifies the active switch processor.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was changed to include the <strong>standby-rp</strong> keyword.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Caution**

When you enter the `attach` or `remote login` command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.
The `module num` keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The `module num` keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the `remote login module num` command, the prompt changes to Router-dfcx# or Switch-sp#, depending on the type of module to which you are connecting.

When you execute the `remote login standby-rp` command, the prompt changes to Router-sdby#.

When you execute the `remote login switch` command, the prompt changes to Switch-sp#.

The `remote login module num` command is identical to the `attach` command.

There are two ways to end the session:

- You can enter the `exit` command as follows:

```
Switch-sp# exit
[Connection to Switch closed by foreign host]
Router#
```

- You can press Ctrl-C three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

### Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch ...  
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the Cisco 7600 series router processor:

```
Router# remote login switch
Trying Switch ...  
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch ...  
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>attach</code></td>
<td>Connects to a specific module from a remote location.</td>
</tr>
</tbody>
</table>
remote-span

To configure a virtual local area network (VLAN) as a remote switched port analyzer (RSPAN) VLAN, use the **remote-span** command in config-VLAN mode. To remove the RSPAN designation, use the **no** form of this command.

```
remote-span
no remote-span
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
This command has no default settings.

**Command Modes**
Config-VLAN mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Cisco 7600 series router.

**Examples**

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Connect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show vlan remote-span</strong></td>
<td>Displays a list of RSPAN VLANs.</td>
</tr>
</tbody>
</table>

rename

To rename a file in a Class C Flash file system, use the **rename** command in EXEC, privileged EXEC, or diagnostic mode.

```
rename url1 url2
```
Syntax Description

<table>
<thead>
<tr>
<th>url1</th>
<th>The original path and filename.</th>
</tr>
</thead>
<tbody>
<tr>
<td>url2</td>
<td>The new path and filename.</td>
</tr>
</tbody>
</table>

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Router and was made available in diagnostic mode.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

In the following example, the file named Karen.1 is renamed test:

Router# dir
Directory of disk0:/Karen.dir/

0 -rw- 0 Jan 21 1998 09:51:29 Karen.1
0 -rw- 0 Jan 21 1998 09:51:29 Karen.2
0 -rw- 0 Jan 21 1998 09:51:29 Karen.3
0 -rw- 0 Jan 21 1998 09:51:31 Karen.4
320492288 bytes total (328400896 bytes free)

Router# rename disk0:/Karen.dir/Karen.1 disk0:/Karen.dir/test

Router# dir
Directory of disk0:/Karen.dir/

0 -rw- 0 Jan 21 1998 09:51:29 Karen.2
0 -rw- 0 Jan 21 1998 09:51:29 Karen.3
0 -rw- 0 Jan 21 1998 09:51:31 Karen.4
254 -rw- 0 Apr 24 1998 09:49:19 test
340492288 bytes total (328384512 bytes free)

request platform software package describe file

To gather descriptive information about an individual module or a Cisco IOS-XE image file, use the request platform software package describe file command in privileged EXEC or diagnostic mode.

request platform software package describe file URL [detail] [verbose]
Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Specifies the URL to the file. The URL contains the file system, directories, and the filename.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies detailed output.</td>
</tr>
<tr>
<td>verbose</td>
<td>Displays verbose information, meaning all information that can be displayed on the console about the file will be displayed.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command can only be used to gather information on individual module and Cisco IOS-XE image files. Using this command to collect information on any other file will generate output, but the generated output is useless.

The output of this command can be used for the following functions:

- To confirm the individual module files that are part of a Cisco IOS-XE image.
- To confirm whether or not a file is bootable.
- To confirm the contexts in which a file must be reloaded or booted.
- To confirm whether or not a file is corrupted.
- To confirm file and header sizes, build dates, and various other general information.

Examples

In the following example, this command is entered to gather information about an individual SIP Base module file on the bootflash: file system.

```
Router# request platform software package describe file
bootflash:asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Package: asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
  Size: 36954316
  Timestamp: 2007-12-05 15:36:27 UTC
  Canonical path: /bootflash/asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg

  Raw disk-file SHA1sum:
    3ee37cdbe276316968866b16df7d8a5733a1502e
  Computed SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Contained SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Hashes match. Package is valid.

  Header size: 204 bytes
  Package type: 10000
  Package flags: 0
```
In the following example, this command is used to gather information about a Cisco IOS-XE image on the bootflash: filesystem.

Router# request platform software package describe file bootflash:ASR1000rp1-advipservicesk9.01.00.12-33.XN.bin
Package: ASR1000rp1-advipservicesk9.01.00.12-33.XN.bin
Size: 21873948
Timestamp: 2007-12-04 17:14:09 UTC
Canonical path: /bootflash/ASR1000rp1-advipservicesk9.01.00.12-33.XN.bin

Raw disk-file SHA1sum:
   d2999fc7e27e01344903a42ffacd62c156eb4acc

Computed SHA1sum:
   5f8cda8518d01d8282d80ecd34f7715783f4a813
Contained SHA1sum:
   5f8cda8518d01d8282d80ecd34f7715783f4a813
Hashes match. Package is valid.

Package is bootable from media and tftp.

Package contents:

Package: asr1000rp1-espbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Size: 52072652
Timestamp: 2007-12-04 13:33:13 UTC

Raw disk-file SHA1sum:
   f1aad6d687256aa327a4e984deab949fbed12b8

Computed SHA1sum:
   15502fd1b8f9fdd4af4014ad4d8026c837929fe6
request platform software package describe file

```
contained SHA1sum:
   15502fd1b8f9ff4af4014ad4d8026c837929fe6
hashes match. Package is valid.
header size: 204 bytes
package type: 20000
package flags: 0
header version: 0

internal package information:
   name: fp
   buildtime: 2007-12-04 05:24
   reldate: Tue 04-Dec-07 01:00
   routeprocessor: rp1
   platform: ASR1000
   user: mcpre
   packagename: espbase
   build: v122_33_xn_asr_rls0_throttle_20071204_051318

package is bootable on ESP when specified by packages provisioning file.

package: asr1000rp1-rpaccess-k9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
size: 21844172
timestamp: 2007-12-04 13:33:01 UTC

raw disk-file SHA1sum:
   025e6159dd91cef9d254ca9fff2602d8ce065939
computed SHA1sum:
eab358324ba5815b9ea623b453a98800ea1c78
contained SHA1sum:
eab358324ba5815b9ea623b453a98800ea1c78
hashes match. Package is valid.
header size: 204 bytes
package type: 30004
package flags: 0
header version: 0

internal package information:
   name: rp_security
   buildtime: 2007-12-04 05:24
   reldate: Tue 04-Dec-07 01:00
   routeprocessor: rp1
   platform: ASR1000
   user: mcpre
   packagename: rpaccess-k9
   build: v122_33_xn_asr_rls0_throttle_20071204_051318

package is not bootable.

package: asr1000rp1-rpbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
size: 21520588
timestamp: 2007-12-04 13:33:06 UTC

raw disk-file SHA1sum:
   432dfa61736d8a51baefbb2d70199d712618dcd2
computed SHA1sum:
83c0335a3adcea574bff237a6c8640a110a045d4
contained SHA1sum:
```

Cisco IOS Configuration Fundamentals Command Reference

412
Hashes match. Package is valid.

Header size: 204 bytes
Package type: 30001
Package flags: 0
Header version: 0

Internal package information:
  Name: rp_base
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rp1
  Platform: ASR1000
  User: mcpre
  PackageName: rpbase
  Build: v122_33_xn_asr_rls0_throttle_20071204_051318

Package is bootable on RP when specified by packages provisioning file.

Package: asr1000rp1-rpcontrol.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Size: 24965324
Timestamp: 2007-12-04 13:33:08 UTC

Raw disk-file SHA1sum:
  eb964b33d4959c21b605d0989e7151cd73488a8f

Computed SHA1sum:
  f1235d703cc422e53bce850c032ff3363b587d70

Hashes match. Package is valid.

Header size: 204 bytes
Package type: 30002
Package flags: 0
Header version: 0

Internal package information:
  Name: rp_daemons
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rp1
  Platform: ASR1000
  User: mcpre
  PackageName: rpcontrol
  Build: v122_33_xn_asr_rls0_throttle_20071204_051318

Package is not bootable.

Package: asr1000rp1-rpios-advipservicesk9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Size: 48515276
Timestamp: 2007-12-04 13:33:13 UTC

Raw disk-file SHA1sum:
  bc13462d6a4af7a817a7346a44a0ef7270e3a81b

Computed SHA1sum:
  f1235d703cc422e53bce850c032ff3363b587d70

Hashes match. Package is valid.
Hashes match. Package is valid.

Header size: 204 bytes
Package type: 30003
Package flags: 0
Header version: 0

Internal package information:
Name: rp_iosd
BuildTime: 2007-12-04_05.24
ReleaseDate: Tue 04-Dec-07 01:00
RouteProcessor: rp1
Platform: ASR1000
User: mcpre
PackageName: rpios-advipservicesk9
Build: v122_33_xn_asr_rls0_throttle_20071204_051318

Package is not bootable.

Package: asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Size: 36954316
Timestamp: 2007-12-04 13:33:11 UTC

Raw disk-file SHA1sum:
3ee37cdbe276316968866b16df7d8a5733a1502e

Computed SHA1sum:
f2db80416a1245a5b1abf2988088860b38ce7898
Contained SHA1sum:
f2db80416a1245a5b1abf2988088860b38ce7898
Hashes match. Package is valid.

Header size: 204 bytes
Package type: 10000
Package flags: 0
Header version: 0

Internal package information:
Name: cc
BuildTime: 2007-12-04_05.24
ReleaseDate: Tue 04-Dec-07 01:00
RouteProcessor: rp1
Platform: ASR1000
User: mcpre
PackageName: sipbase
Build: v122_33_xn_asr_rls0_throttle_20071204_051318

Package is bootable on SIP when specified by packages provisioning file.

Package: asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Size: 19933388
Timestamp: 2007-12-04 13:33:06 UTC

Raw disk-file SHA1sum:
44b6d15cba31fb0e9b27464665ee8a24b92adfd2

Computed SHA1sum:
b1d5faf093b18e196c7c8e1023fe1f7aafdd36d
Contained SHA1sum:
b1d5faf093b18e196c7c8e1023fe1f7aafdd36d
Hashes match. Package is valid.

Header size: 204 bytes
Package type: 10001
Package flags: 0
Header version: 0

Internal package information:
Name: cc_spa
BuildTime: 2007-12-04_05.24
ReleaseDate: Tue 04-Dec-07 01:00
RouteProcessor: rp1
Platform: ASR1000
User: mcpre
PackageName: sipspa
Build: v122_33_xn_asr_rls0_throttle_20071204_051318

Package is not bootable.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>request platform software package install file</td>
<td>Upgrades an individual package or a superpackage file.</td>
</tr>
</tbody>
</table>

**request platform software package expand file**

To extract the individual modules from a Cisco IOS-XE image, use the `request platform software package expand file` command in privileged EXEC or diagnostic mode.

`request platform software package expand file source-URL [to destination-URL] [force] [verbose] [wipe]`

**Syntax Description**

<table>
<thead>
<tr>
<th>source-URL</th>
<th>Specifies the URL to the Cisco IOS-XE file that stores the contents that will be extracted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>to destination-URL</td>
<td>Specifies the destination URL where the files that were extracted from the Cisco IOS-XE file are left after the operation is complete. If this option is not entered, the Cisco IOS-XE image file contents are extracted onto the same directory where the Cisco IOS-XE image file is currently stored.</td>
</tr>
<tr>
<td>force</td>
<td>(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.</td>
</tr>
<tr>
<td>wipe</td>
<td>(Optional) Erases all content on the destination snapshot directory before extracting the files and placing them on the snapshot directory.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC (#)
Diagnostic Mode (diag)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command only extracts individual module files and a provisioning file from the Cisco IOS-XE image. Additional configuration is needed to configure the router to boot using the provisioning files and run using the individual modules.

When this command is used, copies of each module and the provisioning file within the Cisco IOS-XE image are copied and placed on the destination directory. The Cisco IOS-XE image file is unchanged after the operation is complete.

If the `to` destination-URL option is not entered, the Cisco IOS-XE image contents will be extracted onto the same directory where the Cisco IOS-XE image is currently stored.

If this command is used to extract individual module files onto a directory that already contains individual module files, the files that would have been extracted onto the same directory are instead extracted to an automatically created directory on the destination device.

Examples

The following example shows how to extract the individual modules and the provisioning file from a Cisco IOS-XE image that has already been placed in the directory where the user wants to store the individual modules and the provisioning file.

Output of the directory before and after the extraction is given to confirm the files were extracted.

```
Router# dir bootflash:
Directory of bootflash:/
  11 drwx 16384 Dec 4 2007 11:26:07 +00:00 lost+found
14401 drwx 4096 Dec 4 2007 11:27:41 +00:00 .installer
12 -rw- 218783948 Dec 4 2007 12:12:16 +00:00 ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin

Router# request platform software package expand file bootflash:ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin
Verifying parameters
Validating package type
Copying package files

Router# dir bootflash:
Directory of bootflash:/
  11 drwx 16384 Dec 4 2007 11:26:07 +00:00 lost+found
14401 drwx 4096 Dec 4 2007 11:27:41 +00:00 .installer
12 -rw- 218783948 Dec 4 2007 12:12:16 +00:00 ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin
28803 -rw- 52072652 Dec 4 2007 12:14:17 +00:00 asr1000rp1-espbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28804 -rw- 21844172 Dec 4 2007 12:14:17 +00:00 asr1000rp1-rpaccess-k9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28805 -rw- 21520588 Dec 4 2007 12:14:17 +00:00 asr1000rp1-rpbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28806 -rw- 24965324 Dec 4 2007 12:14:19 +00:00 asr1000rp1-rpcontrol.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28807 -rw- 48515276 Dec 4 2007 12:14:20 +00:00 asr1000rp1-rpios-advipservicesk9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28808 -rw- 36954316 Dec 4 2007 12:14:21 +00:00 asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28809 -rw- 19933388 Dec 4 2007 12:14:22 +00:00 asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
28810 -rw- 7145 Dec 4 2007 12:14:22 +00:00 packages.conf
92833536 bytes total (483700736 bytes free)
```
The following example shows how to extract the individual modules and the provisioning file from a Cisco IOS-XE image that has already been placed on the router in a directory that will not store the individual modules and the provisioning file. In this particular example, the contents of a Cisco IOS-XE image stored in usb0: are extracted into bootflash:

Output of the bootflash: directory before and after the extraction is given to confirm the files were extracted.

```
Router# dir usb0:
Directory of usb0:/
1120 -rwx 21325676 Dec 4 2007 10:50:36 +00:00 asr1000rp1-advipservicesk9.v122_33_xn_asr_rls0_throttle.bin

Router# dir bootflash:
Directory of bootflash:/
 11 drwx 16384 Dec 4 2007 12:32:46 +00:00 lost+found
 86401 drwx 4096 Dec 4 2007 14:06:24 +00:00 .ssh
14401 drwx 4096 Dec 4 2007 14:06:36 +00:00 .rollback_timer
43201 drwx 4096 Dec 4 2007 12:34:45 +00:00 .installer

Router# request platform software package expand file usb0:asr1000rp1-advipservicesk9.v122_33_xn_asr_rls0_throttle.bin to bootflash:
Verifying parameters
Validating package type
Copying package files

Router# dir bootflash:
Directory of bootflash:/
 11 drwx 16384 Dec 4 2007 12:32:46 +00:00 lost+found
 86401 drwx 4096 Dec 4 2007 14:06:24 +00:00 .ssh
14401 drwx 4096 Dec 4 2007 14:06:36 +00:00 .rollback_timer
43201 drwx 4096 Dec 4 2007 12:34:45 +00:00 .installer
28803 -rw- 51986636 Dec 4 2007 16:40:38 +00:00 asr1000rp1-espbase.v122_33_xn_asr_rls0_throttle.pkg
28804 -rw- 21838028 Dec 4 2007 16:40:39 +00:00 asr1000rp1-rpaccess-k9.v122_33_xn_asr_rls0_throttle.pkg
28805 -rw- 21508300 Dec 4 2007 16:40:39 +00:00 asr1000rp1-rpbase.v122_33_xn_asr_rls0_throttle.pkg
28806 -rw- 24963276 Dec 4 2007 16:40:40 +00:00 asr1000rp1-rpcontrol.v122_33_xn_asr_rls0_throttle.pkg
28807 -rw- 48419020 Dec 4 2007 16:40:41 +00:00 asr1000rp1-rpios-advipservicesk9.v122_33_xn_asr_rls0_throttle.pkg
28808 -rw- 36946124 Dec 4 2007 16:40:43 +00:00 asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle.pkg
28809 -rw- 14670028 Dec 4 2007 16:40:43 +00:00 asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle.pkg
28802 -rw- 6563 Dec 4 2007 16:40:43 +00:00 packages.conf

928862208 bytes total (708186112 bytes free)
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>request platform software package install file</td>
<td>Upgrades an individual module or a Cisco IOS-XE file.</td>
</tr>
</tbody>
</table>

**request platform software package install commit**

To cancel the rollback timer and commit a software upgrade, use the `request platform software package install commit` command in privileged EXEC or diagnostic mode.
request platform software package install rp rp-slot-number commit [verbose]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp rp-slot-number</td>
<td>Specifies the RP slot number.</td>
</tr>
<tr>
<td>commit</td>
<td>Specifies that an upgrade that was done using a rollback timer that has not expired can be committed.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.</td>
</tr>
</tbody>
</table>

Command Default
No default behavior or values.

Command Modes
Privileged EXEC (#)
Diagnostic Mode (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command is entered after the request platform software package install rp rp-slot-number file command is used with the auto-rollback minutes option to begin an individual sub-package or a consolidated package upgrade. When the auto-rollback minutes option is used in this context, a rollback timer that cancels the upgrade after the number of specified minutes cancels the upgrade if the request platform software package install rp rp-slot-number commit command is not entered to commit the upgrade.

If this command is not entered after the request platform software package install rp rp-slot-number file command is used with the auto-rollback minutes option to upgrade an individual sub-package or a consolidated package and the rollback timer expires, the upgrade does not complete and the router continues running the previous sub-package or consolidated package.

Examples
In the following example, this command is entered to commit an upgrade:

request platform software package install rp 1 commit

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request platform software package install file</td>
<td>Upgrades a consolidated package or sub-package.</td>
</tr>
<tr>
<td>request platform software package install rollback</td>
<td>Rolls back a previous software upgrade.</td>
</tr>
</tbody>
</table>

request platform software package install file

To upgrade a consolidated package or an individual sub-package, use the request platform software package install file command in privileged EXEC or diagnostic mode.

request platform software package install rp rp-slot-number file file-URL [auto-rollback minutes] [provisioning-file URL] [slot slot-number] [bay bay-number] [force] [on-reboot] [verbose]
Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp rp-slot-number</td>
<td>Specifies the route processor (RP) slot number.</td>
</tr>
<tr>
<td>file file-URL</td>
<td>Specifies the URL to the consolidated package or sub-package.</td>
</tr>
<tr>
<td>auto-rollback minutes</td>
<td>Specifies the setting of a rollback timer, and sets the number of minutes on the rollback timer before the rollback timer expires.</td>
</tr>
<tr>
<td>provisioning-file</td>
<td>Specifies the URL to the provisioning file. A provisioning file is used for booting only when a Cisco ASR 1000 Series Aggregation Services Device is booted using individual sub-packages.</td>
</tr>
<tr>
<td>slot slot-number</td>
<td>Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.</td>
</tr>
<tr>
<td>bay bay-number</td>
<td>Specifies the shared port adapter (SPA) bay number within a SIP.</td>
</tr>
<tr>
<td>force</td>
<td>Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.</td>
</tr>
<tr>
<td>on-reboot</td>
<td>Specifies that the installation will not be completed until the next RP reboot.</td>
</tr>
<tr>
<td>verbose</td>
<td>Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.</td>
</tr>
</tbody>
</table>

Command Default

If you do not enter the `request platform software package install file` command, the consolidated or sub package upgrades are not initiated on the device.

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.8S</td>
<td>This command was modified. The <code>mdr</code> keyword was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is used to upgrade consolidated packages and individual sub-packages.

When this command is used to upgrade a SIPBASE sub-package, the `slot slot-number` of the SIP must be specified.

When this command is used to upgrade a SIPSPA sub-package, the `slot slot-number` of the SIP and the `bay bay-number` of the SPA must be specified.

When the `auto-rollback minutes` option is used, the `request platform software package install rp rp-slot-number commit` command must be entered before the rollback timer expires to complete the upgrade. If this command is not entered, the device rolls back to the previous software version. The rollback timer expires after the number of specified `minutes`. If the `auto-rollback minutes` option is not used, the upgrade simply occurs.
Managing and Configuring a consolidated package using the request platform package command

In the following example, the `request platform software package install` command is used to upgrade a consolidated package running on RP 0. The `force` option, which forces the upgrade past any prompt (such as already having the same consolidated package installed), is used in this example.

```
Device# request platform software package install rp 0 file bootflash:ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin force
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
Extracting super package content
Verifying parameters
Validating package type
Copying package files
Checking and verifying packages contained in super package
Creating candidate provisioning file

WARNING: Candidate software will be installed upon reboot
WARNING:

Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
Checking IPC compatibility with running software ... skipped
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned. New software will load on reboot.

Device# reload
```
A reload must be performed to finish this procedure.

SIP Sub-package Installation with Verbose Option

In the following example, the SIP sub-package for the SIP in slot 1 is installed using the `request platform software package install` command. In this example, the `force` option, which forces the upgrade past any prompt (such as already having the same sub-package installed), and the `verbose` option, which displays all possible output during the installation, are used.

```
Device# request platform software package install rp 0 file bootflash:asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle.pkg slot 1 force verbose
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
... file names checked
Verifying image file locations
... image file locations verified
Locating image files and validating name syntax
... image file names validated
Inspecting image file types
... image file types acceptable
Processing image file constraints
... constraints satisfied
Creating candidate provisioning file
... created candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
... verified existing software set is valid
Processing candidate provisioning file
... candidate provisioning file processed
Constructing working set for candidate package set
... working set constructed
Constructing working set for running package set
... working set for running package set constructed
Checking command output
... command output is consistent with command set
Constructing merge of running and candidate packages
... merged running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
... candidate package set is valid
Determining whether installation is valid
Software is unchanged
Software sets are identified as compatible
... installation is valid
```

Checking IPC compatibility with running software

calling minime_merge.sh for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_
minime_merge done for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_

--- Starting candidate package set construction ---
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
... candidate package set is valid
Determining whether installation is valid
Software is unchanged
Software sets are identified as compatible
... installation is valid
Checking IPC compatibility with running software
calling minime_merge.sh for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_
minime_merge done for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_

--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
... candidate package set is valid
Determining whether installation is valid
Software is unchanged
Software sets are identified as compatible
... installation is valid
Checking IPC compatibility with running software
calling minime_merge.sh for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_
minime_merge done for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_

--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
... candidate package set is valid
Determining whether installation is valid
Software is unchanged
Software sets are identified as compatible
... installation is valid
Checking IPC compatibility with running software
calling minime_merge.sh for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_
minime_merge done for /tmp/tdiresolve/compat/_tmp_ISSU_provision_sw_
... IPC is compatible with running software
Checking candidate package set infrastructure compatibility
... candidate package set infrastructure is compatible
Checking infrastructure compatibility with running software
... infrastructure is compatible with running software
Finished compatibility testing
--- Starting impact testing ---
Checking operational impact of change
... operational impact of change is allowable
Finished impact testing
--- Starting commit of software changes ---
Updating provisioning rollback files
... rollback provisioning files updated
Creating pending provisioning file
Ensuring that cached content is written to media
... cached content flushed to media
... pending provisioning file created
Committing provisioning file
Ensuring that cached content is written to media
... cached content flushed to media
... running provisioning file committed
Finished commit of software changes
--- Starting analysis of software changes ---
-------------- changes to running software ------------
0 0 cc
---------------------------------------------------------------------
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
... peer synchronization blocked
Creating the command set placeholder directory
Finding latest command set
... latest command set identified
Assembling CLI output libraries
... CLI output libraries assembled
Assembling CLI input libraries
... CLI input libraries assembled
Applying interim IPC and database definitions
interim IPC and database definitions applied
Replacing running software
... running software replaced
Replacing CLI software
... CLI software replaced
Restarting software
Restarting CC0
Restarting CC0
... software restarted
Applying interim IPC and database definitions
*Oct 9 09:52:25.333: %MCP_OIR-6-OFFLINECARD: Card (cc) offline in slot 0
*Oct 9 09:52:25.334: %MCP_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*Oct 9 09:52:25.334: %MCP_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Oct 9 09:52:25.334: %MCP_OIR-6-REMSPA: SPA removed from subslot 0/2, interfaces disabled
*Oct 9 09:52:25.334: %MCP_OIR-6-REMSPA: SPA removed from subslot 0/3, interfaces disabled
... interim IPC and database definitions applied
Notifying running software of updates
... running software notified
Unblocking peer synchronization of operating information
... peer synchronization unblocked
... unmount of old packages scheduled
Unmounting old packages
... inactive old packages unmounted
Cleaning temporary installation files
... temporary installation files cleaned
Finished update running software
SUCCESS: Finished installing software.
Device#

Upgrading SIP Sub-package without using the verbose option

In the following example, the SIP sub-package for the SIP in slot 1 is installed using the `request platform software package install` command. In this example, the `force` option, which forces the upgrade past any prompt (such as already having the same sub-package installed), is used. The `verbose` option is not used in this example.

Device# request platform software package install rp 0 file bootflash:asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle.pkg slot 1 force
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Software sets are identified as compatible
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Finished compatibility testing
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
Finding latest command set
Assembling CLI output libraries
Assembling CLI input libraries
Applying interim IPC and database definitions
   interim IPC and database definitions applied
   Replacing running software
   Replacing CLI software
   Restarting software
Restarting CC1
Restarting CC1
   Applying interim IPC and database definitions
   *Oct  9 09:54:55.365: %MCP_OIR-6-OFFLINECARD: Card (cc) offline in slot 1
   *Oct  9 09:54:55.365: %MCP_OIR-6-REMSPA: SPA removed from subslot 1/1, interfaces disabled
   *Oct  9 09:54:55.365: %MCP_OIR-6-REMSPA: SPA removed from subslot 1/2, interfaces disabled
Notifying running software of updates
Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
Finished update running software
SUCCESS: Finished installing software.
Device#

Upgrading IOS Sub-package
In the following example, the request platform software package install command is used to upgrade an IOS sub-package. In this example, the force option, which forces the upgrade past any prompt (such as already having the same module installed), is used.

Device# request platform software package install rp 0 file bootflash:asr1000rp1-rpios-advipservicesk9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
   force

   --- Starting installation state synchronization ---
   Finished installation state synchronization
   --- Starting file path checking ---
   Finished file path checking
   --- Starting image file verification ---
   Checking image file names
   Verifying image file locations
   Locating image files and validating name syntax
   Inspecting image file types
       WARNING: In-service installation of IOSD package
       WARNING: requires software redundancy on target RP
       WARNING: or on-reboot parameter
       WARNING: Automatically setting the on-reboot flag
   Processing image file constraints
   Creating candidate provisioning file
   Finished image file verification
   --- Starting candidate package set construction ---
   Verifying existing software set
   Processing candidate provisioning file
   Constructing working set for candidate package set
   Constructing working set for running package set
   Checking command output
   Constructing merge of running and candidate packages
   Finished candidate package set construction
   --- Starting compatibility testing ---
   Determining whether candidate package set is compatible
   WARNING:
WARNING: Candidate software combination not found in compatibility database

WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned. New software will load on reboot.

Device#

Note that the new RPIOS sub-package will become active only after a reboot. Reboot the device to finish this procedure.

Upgrading SPA Sub-package

In the following example, the request platform software package install command is use to upgrade a SIPSPA sub-package for the SPA in bay 0 of device slot 1. In this example, the force option, which forces the upgrade past any prompt (such as already having the same module installed), is used.

```
Device# request platform software package install rp 0 file
bootflash:asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg slot 1 bay 0 force

--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Software sets are identified as compatible
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
```
Finished compatibility testing
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
Finding latest command set
Assembling CLI output libraries
Assembling CLI input libraries
Applying interim IPC and database definitions
interim IPC and database definitions applied
Replacing running software
Replacing CLI software
Restarting software
Restarting SPA CC1/0
Applying interim IPC and database definitions
Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
Finished update running software
SUCCESS: Finished installing software.

Device# request platform software package install rollback

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>request platform software package install</td>
<td>Cancels the rollback timer and commits a software upgrade.</td>
</tr>
<tr>
<td></td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>request platform software package install</td>
<td>Rolls back a previous software upgrade.</td>
</tr>
<tr>
<td></td>
<td>rollback</td>
<td></td>
</tr>
<tr>
<td></td>
<td>request platform software package install</td>
<td>Creates a snapshot directory that will contain all the files extracted from</td>
</tr>
<tr>
<td></td>
<td>snapshot</td>
<td>a consolidated package.</td>
</tr>
</tbody>
</table>

**request platform software package install rollback**

To roll back a previous software upgrade, use the `request platform software package install rollback` command in privileged EXEC or diagnostic mode.

```plaintext
request platform software package install rp rp-slot-number rollback [{as-booted|provisioning-file provisioning-file-URL}] [force] [on-reboot] [verbose]
```

**Syntax Description**

- `rp` rp-slot-number: Specifies the slot number of the RP doing the request.
- `as-booted`: Specifies that the software update will not occur, and that the router will instead boot using the same procedure that it used during the last bootup.
request platform software package install snapshot

To create a snapshot directory that contains all the files extracted from a consolidated package, use the `request platform software package install snapshot` command in privileged EXEC or diagnostic mode.

```
request platform software package install rp rp-slot-number snapshot to URL [as snapshot-provisioning-filename] [force] [verbose] [wipe]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rp</code> <code>rp-slot-number</code></td>
<td>Specifies the slot number.</td>
</tr>
</tbody>
</table>
The `request platform software package install snapshot` command is used to create a directory at the destination device and extract the individual sub-packages from a consolidated package to that directory.

**Usage Guidelines**

This command is used to create a directory at the destination device and extract the individual sub-packages in a consolidated package to that directory.

The `request platform software package expand` command is the only other command that can be used to extract individual sub-packages from a consolidated package.

**Examples**

In the following example, a snapshot directory named `snapdir1_snap` is created in the `bootflash:` file system, and the individual sub-package files from the consolidated package are extracted into the snapshot directory.

The second portion of the example first sets up the router to reboot using the files in the snapshot directory (deletes all previous boot system commands, configures the configuration register, then enters a boot system command to boot using the extracted provisioning file), saves the new configuration, then reboots so the router will boot using the extracted provisioning file, which allows the router to run using the extracted individual sub-package files.

```bash
Router(diag)# request platform software package install rp 0 snapshot to bootflash:snapdir1_snap
--- Starting active image file snapshot --- Validating snapshot parameters Creating destination directory Copying files to destination media
```
Copied provisioning file as packages.conf
Copying package file asr1000rp1-rpbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Copying package file asr1000rp1-rpcontrol.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Copying package file asr1000rp1-rpios-advipservicesk9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Copying package file asr1000rp1-rpaccess-k9.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Copying package file asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Copying package file asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg
Copying package file asr1000rp1-espbase.v122_33_xn_asr_rls0_throttle_20071204_051318.pkg

Moving files into final location Finished active image file snapshot
Router(config)# no boot system
Router(config)# config-register 0x1
Router(config)# boot system harddisk: snapdir1_snap/packages.conf
Router(config)# exit
*May 11 01:31:04.815: %SYS-5-CONFIG_I: Configured from console by con
Router# write mem
Building configuration...
[OK]

Router# reload

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>request platform software process release</code></td>
<td>Upgrades a consolidated package or an individual sub-package.</td>
</tr>
</tbody>
</table>

**request platform software process release**

To restart processes that have been placed in the hold down state by the Process Manager on the Cisco ASR 1000 Series Routers, use the `request platform software process release` command in privileged EXEC or diagnostic mode.

`request platform software process release slot all`
Syntax Description

<table>
<thead>
<tr>
<th>slot</th>
<th>Specifies the hardware slot. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• number -- The number of the SIP slot of the hardware module where the trace level is being set.</td>
</tr>
<tr>
<td></td>
<td>For instance, if you wanted to specify the SIP in SIP slot 2 of the router, enter 2 as the number.</td>
</tr>
<tr>
<td></td>
<td>• f0 -- The ESP in ESP slot 0.</td>
</tr>
<tr>
<td></td>
<td>• f1 -- The ESP in ESP slot 1</td>
</tr>
<tr>
<td></td>
<td>• fp active -- The active ESP.</td>
</tr>
<tr>
<td></td>
<td>• fp standby -- The standby ESP.</td>
</tr>
<tr>
<td></td>
<td>• r0 -- The RP in RP slot 0.</td>
</tr>
<tr>
<td></td>
<td>• r1 -- The RP in RP slot 1.</td>
</tr>
<tr>
<td></td>
<td>• rp active -- The active RP.</td>
</tr>
<tr>
<td></td>
<td>• rp standby -- The standby RP.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all processes currently in the holddown state within the selected slot will be restarted.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#) Diagnostic Mode (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is used to restart processes in the holddown state. If a process is in the holddown state, a console message is generated to notify the user that the process is holddown.

Before placing any process in the holddown state, the Process Manager makes up to 5 attempts over 120 seconds to enable the process. These attempts to enable the process also happen automatically at startup. If the Process Manager is unable to enable the process after these attempts, the process will then be placed in the holddown state.

When this command is entered, it only attempts to restart processes currently in the holddown state. Active processes will not be affected by entering this command.

Examples

In the following example, this command is entered to restart any process currently on RP 0 in the holddown state:

```
request platform software process release r0 all
```

**request platform software system shell**

To request platform shell access, use the `request platform software system shell` command in privileged EXEC mode.
request platform software system shell [{rp|esp|sip}]

**Syntax Description**

- **rp**: Specifies the Route Processor (RP); it can be either active or standby.
- **esp**: Specifies the Embedded Services Processor (ESP) control processor; it can be either active or standby.
- **sip**: Specifies the SPA Interface Processor (SIP).

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)XNC</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The platform shell command needs to be entered before using the request platform software system shell command. Providing shell access would not be necessary. However, there might be some cases where the command may not be available, or the IOS process hangs, or IOS console may not be available. In such cases, you can login to the shell and see the status of the system.

The shell should be accessed under Cisco supervision, and no support is provided if accessed without supervision. The following message is displayed, before the shell access is granted:

"Activity within this shell can jeopardize the functioning of the system.
Use this functionality only under supervision of Cisco Support."

**Examples**

In the following example,

```
Router(config)# platform shell
Router(config)# exit
Router(config)# request platform software shell system
Activity within this shell can jeopardize the functioning of the system.
Are you sure you want to continue? [y/n] y
******************************************************************************
Activity within this shell can jeopardize the functioning of the system.
Use this functionality only under supervision of Cisco Support.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>platform shell</td>
<td>Grants shell and enters shell access grant configuration mode.</td>
</tr>
</tbody>
</table>

**request platform software shell session output format**

To modify the format of the output of some `show` commands on the Cisco ASR1000 Series Routers, use the `request platform software shell session output format` command in privileged EXEC and diagnostic mode.

```
request platform software shell session output format format
```
Syntax Description

<table>
<thead>
<tr>
<th>format</th>
<th>Specifies the output format for show command output. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td>html</td>
<td>Specifies Hypertext Markup Language (HTML) output.</td>
</tr>
<tr>
<td>raw</td>
<td>Specifies the raw message output.</td>
</tr>
<tr>
<td>text</td>
<td>Specifies plaintext output, which is the default.</td>
</tr>
<tr>
<td>xml</td>
<td>Specifies Extensible Markup Language (XML) output</td>
</tr>
</tbody>
</table>

Command Default

All show command output is seen in plaintext (the text format) by default.

Command Modes

Privileged EXEC (#) Diagnostic Mode (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE Release 2.1</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

Usage Guidelines

Entering this command can only change the output of some show commands that are available in both privileged EXEC and diagnostic mode. At the current time, most of these commands are show platform software and show platform hardware commands.

Only a small subset of commands currently produce output using the html option.

Examples

In the following example, the request platform software shell session output format command is used to change the show output format from text to raw. The output of the show platform hardware slot r0 alarms visual command is shown both before and after the request platform software shell session output format command was entered to illustrate the change in output format.

Router# show platform hardware slot r0 alarms visual

Current Visual Alarm States
Critical: On
Major: On
Minor: Off

Router# request platform software shell session output format raw

Router# show platform hardware slot r0 alarms visual

message@alarms_msg: {
    tdl_cman_alarms_data@tdl_cman_alarms_data: {
        critical@tdl_boolean: TDL_TRUE
        major@tdl_boolean: TDL_TRUE
        minor@tdl_boolean: TDL_FALSE
    }
}

message@ui_req_msg: {
    ui_req@ui_req: {
        request_id@U64:2
        client@ui_client: {
            location@svc_loc: {
                fru@fru:BINOS_FRU_RP
                slotnum@I16:0
                baynum@I16:0
            }
            client_type@ui_client_type:UIClient_INVALID
            term_type@ui_terminal_type:UITT_INVALID
        }
    }
}
In the following example, the request platform software shell session output format command is used to change the show output format from text to xml. The output of the show platform hardware slot r0 alarms visual command is shown both before and after the request platform software shell session output format command was entered to illustrate the change in output format.

Router# show platform hardware slot r0 alarms visual
Current Visual Alarm States
Critical: On
Major : On
Minor : Off
Router# request platform software shell session output format xml
Router# show platform hardware slot r0 alarms visual

<?xml version="1.0"?>
<iossr-response action="3">
  <cmd-response>
    <alarms_msg>
      <tdl_cman_alarms_data>
        <critical><TDL_TRUE/></critical>
        <major><TDL_TRUE/></major>
        <minor><TDL_FALSE/></minor>
      </tdl_cman_alarms_data>
      <ui_req_msg>
        <ui_req>
          <request_id>4</request_id>
          <client>
            <location>
              <fru><BINOS_FRU_RP/></fru>
            </location>
            <slotnum>0</slotnum>
            <baynum>0</baynum>
          </client>
          <client_type><UICLIENT_INVALID/></client_type>
          <term_type><UITT_INVALID/></term_type>
        </ui_req>
      </ui_req_msg>
    </alarms_msg>
  </cmd-response>
</iossr-response>

request platform software snapshot
To take a snapshot of the bootflash, use the request platform software snapshot command in privilege EXEC mode.

request platform software snapshot slot {cancel|create|delete|restore}name

Syntax Description

| snapshot | Requests snapshot actions. |
**request platform software snapshot**

- **slot**
  - Specifies the hardware slot. Options include:
    - **number** -- The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you wanted to specify the SIP in SIP slot 2 of the router, enter 2 as the number.
    - **f0** -- The ESP in ESP slot 0.
    - **f1** -- The ESP in ESP slot 1
    - **fp active** -- The active ESP.
    - **fp standby** -- The standby ESP.
    - **r0** -- The RP in RP slot 0.
    - **r1** -- The RP in RP slot 1.
    - **rp active** -- The active RP.
    - **rp standby** -- The standby RP.

- **cancel**
  - Cancels a snapshot operation.

- **create**
  - Creates a snapshot.

- **delete**
  - Deletes a snapshot.

- **restore**
  - Restores a snapshot.

- **name**
  - Specifies the name of the snapshot to be modified.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC (#) Diagnostic Mode (diag)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **request platform software snapshot** command to create a snapshot of the bootflash, including the NVRAM partitions and the ROMMON memory, on the harddisk. This command can also be used to restore a snapshot.

**Examples**

This example shows how to create a snapshot named "stan" on the processor in the RO slot.

```
router#request platform software snapshot R0 create stan
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform software snapshot status</td>
<td>Use this command to display a snapshot of the bootflash.</td>
</tr>
</tbody>
</table>
request platform software vty attach

To enter EXEC mode on a router after persistent SSH or persistent Telnet is configured to connect to the router in diagnostic mode, use the request platform software vty attach command in diagnostic mode.

request platform software vty attach [permanent]

Syntax Description

| permanent | (Optional) Specifies that the router should not return to diagnostic mode if EXEC mode is exited. |

Command Default

No default behavior or values

Command Modes

Diagnostic (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If persistent Telnet or persistent SSH is configured to make users wait for an IOS vty line before allowing them to access the IOS CLI, this command can be used to attach to an IOS vty line and place the user in EXEC mode. Exiting EXEC mode returns the user to diagnostic mode unless the permanent keyword is entered. When the permanent keyword is entered, exiting EXEC mode exits the router.

The vty lines must be configured to allow local login for this command to work. The vty lines must also be configured to accept the type of transport traffic (SSH or Telnet) being used to connect to the router for the session in which the request platform software vty attach command is entered.

Examples

In the following example, this command is used to leave diagnostic mode and enter privileged EXEC mode:

Router(diag) #
request platform software vty attach
Router#

In the following example, this command is used to leave diagnostic mode and enter privileged EXEC mode. The user then re-enters diagnostic mode by exiting privileged EXEC mode:

Router(diag) # request platform software vty attach
Router# exit
Router(diag) #

In the following example, this command is used with the permanent option to leave diagnostic mode and enter privileged EXEC mode. The user then exits the router by exiting privileged EXEC mode:

Router(diag) # request platform software vty attach permanent
Router# exit
Connection to Router closed.
To set the revision number for the Multiple Spanning Tree (802.1s) (MST) configuration, use the `revision` command in MST configuration submode. To return to the default settings, use the `no` form of this command.

```
revision  version
no  revision
```

**Syntax Description**

```
version  Revision number for the configuration; valid values are from 0 to 65535.
```

**Command Default**

```
version  is 0
```

**Command Modes**

MST configuration (config-mst)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Two Cisco 7600 series routers that have the same configuration but different revision numbers are considered to be part of two different regions.

**Caution**

Be careful when using the `revision` command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

**Examples**

This example shows how to set the revision number of the MST configuration:

```
Router(config-mst)#  revision  5
Router(config-mst)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Maps a VLAN or a set of VLANs to an MST instance.</td>
</tr>
<tr>
<td>name (MST configuration submode)</td>
<td>Sets the name of an MST region.</td>
</tr>
<tr>
<td>show</td>
<td>Verifies the MST configuration.</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>Displays information about the spanning-tree state.</td>
</tr>
<tr>
<td>spanning-tree mst configuration</td>
<td>Enters MST-configuration submode.</td>
</tr>
</tbody>
</table>
**rmdir**

To remove an existing directory in a Class C Flash file system, use the `rmdir` command in EXEC, privileged EXEC, or diagnostic mode.

```
rmdir directory
```

**Syntax Description**

- `directory` Directory to delete.

**Command Modes**

- User EXEC
- Privileged EXEC
- Diagnostic

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR1000 Series Router and was made available in diagnostic mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is valid only on Class C Flash file systems.

**Caution**

You can use the `rmdir` command to remove a directory that another user is currently accessing in read-only mode, for example if it is that user’s default working directory. If you use the `rmdir` command to remove such a directory and a user whose current directory is set to the deleted directory then uses the `pwd` command to display the current working directory, the following error message is displayed: Cannot determine current directory.

**Examples**

The following example deletes the directory named `newdir`:

```
Router# dir
Directory of flash:
  2 drwx 0 Mar 13 1993 13:16:21 newdir
8128000 bytes total (8126976 bytes free)
Router# rmdir newdir
Rmdir file name [newdir]?
Delete flash:newdir? [confirm]
Removed dir flash:newdir
Router# dir
Directory of flash:
No files in directory
8128000 bytes total (8126976 bytes free)
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dir</strong></td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td><strong>mkdir</strong></td>
<td>Creates a new directory in a Class C Flash file system.</td>
</tr>
</tbody>
</table>

### rommon-pref

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR router or Cisco 7301 router when you are in ROMmon, use the **rommon-pref** command in ROM monitor mode.

```
rommon-pref [readonly|upgrade]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>readonly</strong></td>
<td>Selects the ReadOnly ROMmon image to be booted on the next reload.</td>
</tr>
<tr>
<td><strong>upgrade</strong></td>
<td>Selects the Upgrade, second ROMmon image to be booted on the next reload.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

ROM monitor mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(28)S</td>
<td>This command was introduced on the Cisco 7200 VXR router. It was introduced in ROMmon version 12.3(4r)T1 for the Cisco 7200 VXR router.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router. It was introduced in ROMmon version 12.3(4r)T2 for the Cisco 7301 router.</td>
</tr>
<tr>
<td>12.3(9)</td>
<td>This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You might select the ReadOnly ROMmon image to be booted on the next reload because the Upgrade image has features or side effects you do not like.

When you are in ROMmon, there is no descriptive output to inform you whether the ReadOnly ROMmon image was reloaded. To confirm the reload, use the showmon command after entering the rommon-pref readonly command.

Use this command when you are in ROMmon mode. Use the **upgrade rom-monitor preference** command when you are in Cisco IOS.

**Examples**

The following example, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, shows how to select the ReadOnly ROMmon image to be booted on the next reload of the router when you are already in ROMmon mode:

```
rommon 2 > rommon-pref readonly
```
route-converge-interval

To configure the time interval after which the old FIB entries are purged, use the `route-converge-interval` command in main CPU submode. To return to the default settings, use the `no` form of this command.

```
route-converge-interval  seconds
no  route-converge-interval
```

**Syntax Description**

| seconds | Time interval, in seconds, after which the old FIB entries are purged; valid values are from 60 to 3600 seconds. |

**Command Default**

`seconds` is 120 seconds (2 minutes).

**Command Modes**

Main CPU submode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17b)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command is supported on releases prior to Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SRM/SSO is supported in the following releases only.

- Release 12.2(17b)SX and later rebuilds of Release 12.2(17b)SXA
- Release 12.2(17d)SX and later rebuilds of Release 12.2(17d)SXB

This command is not supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The time interval for route-converge delay is needed to simulate the route-converge time when routing protocols restart on switchover.

**Examples**

This example shows how to set the time interval for the route-converge delay:

```
Router(config) # redundancy
Router(config-red) # main-cpu
Router(config-red-main) # route-converge-interval 90
Router(config-red-main) #
```

This example shows how to return to the default time interval for the route-converge delay:

```
Router(config) # redundancy
Router(config-red) # main-cpu
```
Router(config-red-main)# no route-converge-interval
Router(config-red-main)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>redundancy</td>
<td>Enters redundancy configuration mode.</td>
</tr>
</tbody>
</table>

**rsh**

To execute a command remotely on a remote shell protocol (rsh) host, use the `rsh` command in privileged EXEC mode.

```
rsh {ip-address host} [/user username] remote-command
```

**Syntax Description**

- **ip-address**
  - IP address of the remote host on which to execute the `rsh` command. Either the IP address or the host name is required.

- **host**
  - Name of the remote host on which to execute the command. Either the host name or the IP address is required.

- **/user username**
  - (Optional) Remote username.

- **remote-command**
  - Command to be executed remotely.

**Command Default**

If you do not specify the `/user username` keyword and argument, the Cisco IOS software sends a default remote username. As the default value of the remote username, the software sends the username associated with the current tty process, if that name is valid. For example, if the user is connected to the router through Telnet and the user was authenticated through the `username` command, then the software sends that username as the remote username. If the tty username is invalid, the software uses the host name as the both the remote and local usernames.

**Note**

For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are sometimes called tty devices (tty stands for teletype, the original UNIX terminal).

**Command Modes**

- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `rsh` command to execute commands remotely. The host on which you remotely execute the command must support the rsh protocol, and the `.rhosts` files on the rsh host must include an entry that permits you to remotely execute commands on that host.
For security reasons, the software does not default to a remote login if no command is specified, as does UNIX. Instead, the router provides Telnet and connect services that you can use rather than rsh.

**Examples**

The following command specifies that the user named sharon attempts to remotely execute the UNIX `ls` command with the `-a` argument on the remote host named mysys.cisco.com. The command output resulting from the remote execution follows the command example:

```
Router1# rsh mysys.cisco.com /user sharon ls -a
.
.
.alias
.cshrc
.emacs
.exrc
.history
.login
.mailrc
.newsrc
.oldnewsrc
.rhosts
.twmrc
.xsession
.jazz
```

**scheduler allocate**

To guarantee CPU time for processes, use the `scheduler allocate` command in global configuration mode. To restore the default, use the `no` form of this command.

```
scheduler allocate interrupt-time process-time
no scheduler allocate
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>interrupt-time</td>
<td>Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is from 400 to 60000 microseconds. The default is 4000 microseconds.</td>
</tr>
<tr>
<td>process-time</td>
<td>Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is from 100 to 4000 microseconds. The default is 200 microseconds. The default for Catalyst 6500 series switches and Cisco 7600 series routers is 800 microseconds.</td>
</tr>
</tbody>
</table>

**Command Default**

Approximately 5 percent of the CPU is available for process tasks.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>
Modification

This command was changed as follows:

- The process-time default setting was changed from 200 microseconds to 800 microseconds.
- The no scheduler allocate action was changed to return to the default settings.

12.2(17a)SX

Support for this command on the Supervisor Engine 2 was extended to the 12.2(17d)SXB release.

12.2(17d)SXB

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

Usage Guidelines

This command applies to the Catalyst 6500 series switches, Cisco 7200 series, Cisco 7500 series, and Cisco 7600 series routers.

Caution

We recommend that you do not change the default settings. Changing settings associated with CPU processes can negatively impact system performance.

Examples

The following example makes 20 percent of the CPU available for process tasks:

Router(config)# scheduler allocate 2000 500

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler interval</td>
<td>Controls the maximum amount of time that can elapse without running system processes.</td>
</tr>
</tbody>
</table>

scheduler heapcheck enable

To enable heapcheck processing, use the scheduler heapcheck enable command in global configuration mode. To disable scheduler heapcheck processing, use the no form of this command.

scheduler heapcheck enable
no scheduler heapcheck enable

Syntax Description

This command has no arguments or keywords.

Command Default

The scheduler heapcheck enable command is disabled by default. If no keywords are specified, scheduler heapcheck processing will not be performed.

Command Modes

Global configuration (config)
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T</td>
<td>This command was introduced in the Cisco IOS Release 15.2(1)T.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable scheduler heapcheck processing:

```
Router# configure terminal
Router(config)# scheduler heapcheck enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler heapcheck process</td>
<td>Performs a sanity check for corruption in memory blocks when a process switch occurs.</td>
</tr>
</tbody>
</table>

**scheduler heapcheck poll**

To validate the memory and edism poll routine, use the `scheduler heapcheck poll` command in global configuration mode. To disable the memory check and edism poll routine, use the `no` form of this command.

```
scheduler heapcheck poll
no scheduler heapcheck poll
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The `scheduler heapcheck poll` command is disabled by default. If no keywords are specified, a sanity check is performed on all the memory blocks and memory pools.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to validate the memory check and edism poll routine:

```
Router# configure terminal
Router(config)# scheduler heapcheck poll
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler heapcheck process</td>
<td>Performs a sanity check for corruption in memory blocks when a process switch occurs.</td>
</tr>
</tbody>
</table>
scheduler heapcheck process

To perform a “sanity check” for corruption in memory blocks when a process switch occurs, use the scheduler heapcheck process command in global configuration mode. To disable this feature, use the no form of this command.

```
 scheduler heapcheck process [memory [fast] [io] [multibus] [pci] [processor] [checktype {all|data|magic|mlite-data|pointer|refcount|lite-chunks}]]
 no scheduler heapcheck process
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>(Optional) Specifies checking all memory blocks and memory pools.</td>
</tr>
<tr>
<td>fast</td>
<td>(Optional) Specifies checking the fast memory block.</td>
</tr>
<tr>
<td>io</td>
<td>(Optional) Specifies checking the I/O memory block.</td>
</tr>
<tr>
<td>multibus</td>
<td>(Optional) Specifies checking the multibus memory block.</td>
</tr>
<tr>
<td>pci</td>
<td>(Optional) Specifies checking the process control information (PCI) memory block.</td>
</tr>
<tr>
<td>processor</td>
<td>(Optional) Specifies checking the processor memory block.</td>
</tr>
<tr>
<td>checktype</td>
<td>(Optional) Specifies checking specific memory pools.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Specifies checking the value of the block magic, red zone, size, refcount, and pointers (next and previous).</td>
</tr>
<tr>
<td>data</td>
<td>(Optional) Specifies checking the value of normal blocks.</td>
</tr>
<tr>
<td>magic</td>
<td>(Optional) Specifies checking the value of the block magic, red zone, and size.</td>
</tr>
<tr>
<td>mlite-data</td>
<td>(Optional) Specifies checking the value of memory allocation lite (malloc-lite) blocks.</td>
</tr>
<tr>
<td>pointer</td>
<td>(Optional) Specifies checking the value of the next and previous pointers.</td>
</tr>
<tr>
<td>refcount</td>
<td>(Optional) Specifies checking the value of the block magic and refcount.</td>
</tr>
<tr>
<td>lite-chunks</td>
<td>(Optional) Specifies checking the memory blocks allocated by the memory allocation lite (malloc_lite) feature.</td>
</tr>
</tbody>
</table>

### Command Default

This command is disabled by default. If no keywords are specified, a sanity check will be performed on all the memory blocks and memory pools.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The lite-chunks keyword was added.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The data and mlite-data keywords were added.</td>
</tr>
</tbody>
</table>
Usage Guidelines

When configuring this command, you can choose none or all memory block keywords (fast, io, multibus, pci, processor, and checktype).

Enabling this command has a significant impact on router performance.

Examples

The following example shows how to sanity check for corruption in the I/O memory block when a process switch occurs. In this example, the values of only the block magic, red zone, and size will be checked.

```
scheduler heapcheck process memory io checktype magic
```

The following example shows how to sanity check for corruption in the processor memory block when a process switch occurs. In this example, the values of only the next and previous pointers will be checked.

```
scheduler heapcheck process memory processor checktype pointer
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory lite</td>
<td>Enables the malloc_lite feature.</td>
</tr>
<tr>
<td>memory sanity</td>
<td>Performs a “sanity check” for corruption in buffers and queues.</td>
</tr>
</tbody>
</table>

scheduler interrupt mask profile

To start interrupt mask profiling for all processes running on the system, use the `scheduler interrupt mask profile` command in global configuration mode. To stop interrupt mask profiling, use the `no` form of this command.

```
scheduler interrupt mask profile
no scheduler interrupt mask profile
```

Syntax Description

This command has no arguments or keywords.

Command Default

Interrupt mask profiling is disabled by default.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command enables the collection of details regarding the total amount of time a process has masked interrupts since the interrupt mask profiler was enabled.

Examples

The following example shows how to enable interrupt mask profiling:

```
Router(config)# scheduler interrupt mask profile
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear processes interrupt mask detail</td>
<td>Clears the interrupt masked details for all processes and stack traces that have been dumped into the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask size</td>
<td>Configures the maximum number of entries that can exist in the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask time</td>
<td>Configures the maximum allowed time that a process can run with interrupts masked.</td>
</tr>
<tr>
<td>show process interrupt mask buffer</td>
<td>Displays the information stored in the interrupt mask buffer.</td>
</tr>
<tr>
<td>show processes interrupt mask detail</td>
<td>Displays interrupt masked details for the specified process or all processes in the system.</td>
</tr>
</tbody>
</table>

scheduler interrupt mask size

To configure the maximum number of entries that can exist in the interrupt mask buffer, use the scheduler interrupt mask size command in global configuration mode. To reset the maximum number of entries that can exist in the interrupt mask buffer to the default, use the no form of this command.

```
scheduler interrupt mask size buffersize
no scheduler interrupt mask size
```

Syntax Description

buffersize | Specifies the number of entries that can exist in the interrupt mask buffer.

Command Default

The default buffer size is 50 entries.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure 100 entries the maximum number of entries that can exist in the interrupt mask buffer:

```
Router(config)# scheduler interrupt mask size 100
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear processes interrupt mask detail</td>
<td>Clears the interrupt masked details for all processes and stack traces that have been dumped into the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask profile</td>
<td>Enables or disables interrupt mask profiling for all processes running on the system.</td>
</tr>
</tbody>
</table>
### scheduler interrupt mask time

To configure the maximum time that a process can run with interrupts masked before another entry is created in the interrupt mask buffer, use the `scheduler interrupt mask time` command in global configuration mode. To reset the threshold time to the default, use the `no` form of this command.

```plaintext
scheduler interrupt mask time threshold-time
no scheduler interrupt mask time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>threshold-time</code></td>
<td>Specifies the maximum amount of time in microseconds a process can be in interrupt masked state without creating an entry in the interrupt mask buffer.</td>
</tr>
</tbody>
</table>

**Command Default**

The default threshold time value is 50 microseconds.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following shows how to configure 100 microseconds as the maximum time a process can run with interrupts masked before another entry is created in the interrupt mask buffer:

```plaintext
Router(config)# scheduler interrupt mask time 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear processes interrupt mask detail</td>
<td>Clears the interrupt masked details for all processes and stack traces that have been dumped into the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask profile</td>
<td>Enables or disables interrupt mask profiling for all processes running on the system.</td>
</tr>
<tr>
<td>scheduler interrupt mask size</td>
<td>Configures the maximum number of entries that can exist in the interrupt mask buffer.</td>
</tr>
</tbody>
</table>
### scheduler interval

To control the maximum amount of time that can elapse without running system processes, use the `scheduler interval` command in global configuration mode. To restore the default, use the `no` form of this command.

`scheduler interval milliseconds`  
`no scheduler interval`

**Syntax Description**

| milliseconds | Integer that specifies the interval (in milliseconds). The minimum interval that you can specify is 500 milliseconds; there is no maximum value. |

**Command Default**

High-priority operations are allowed to use as much of the CPU as needed.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The normal operation of the network server allows the switching operations to use as much of the central processor as is required. If the network is running unusually heavy loads that do not allow the processor the time to handle the routing protocols, give priority to the system process scheduler. High-priority operations are allowed to use as much of the CPU as needed.

**Note**

Changing settings associated with CPU processes can negatively impact system performance.

On the Cisco 7200 series and Cisco 7500 series, use the `scheduler allocate` global configuration command instead of the `scheduler interval` command.

**Examples**

The following example changes the low-priority process schedule to an interval of 750 milliseconds:

```
Router(config)# scheduler interval 750
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler allocate</td>
<td>Guarantees CPU time for processes.</td>
</tr>
</tbody>
</table>
scheduler isr-watchdog

To detect if an Interrupt Service Routine (ISR) is suspended or stalled and to schedule and manage a watchdog timeout on an ISR, use the scheduler isr-watchdog command in global configuration mode. To disable the configuration, use the no form of this command.

```
scheduler isr-watchdog
no scheduler isr-watchdog
```

**Syntax Description**
There are no additional keywords or arguments with this command.

**Command Default**
The default detection time is 2 minutes.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The timer ISR checks the current context to avoid holding processes accountable for CPU time spent servicing interrupts during the process time slice, and vice versa for interrupt-level code accountability. However, at each timer tick, the timer ISR applies the full 4 milliseconds of CPU time to the current context. As a result, depending on when the timer tick occurs in relation to a context switch, you might see inaccuracies in CPU utilization accounting compared with the actual computation time because some or all of the tick is being applied to the wrong context.

**Examples**
The following example shows how to detect if an ISR is suspended or stalled and to manage a watchdog timeout on an ISR:

```
Router> enable
Router# configure terminal
Router(config)# scheduler isr-watchdog
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler max-sched-time</td>
<td>Configures the maximum time in milliseconds that a scheduler can run without flagging an error.</td>
</tr>
</tbody>
</table>

scheduler max-sched-time

To configure or change the maximum time, in milliseconds that a scheduler can run without flagging an error or overload of the CPU, use the scheduler max-sched-time command in global configuration mode. To disable this configuration, use the no form of this command.

```
scheduler max-sched-time milliseconds
no scheduler max-sched-time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>milliseconds</th>
<th>The maximum time, in milliseconds (ms). The range is from 1 to 3600.</th>
</tr>
</thead>
</table>
Command Default

The default time is 2000 ms to signal an overload of the CPU.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(1)M.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The default behavior of the `scheduler max-sched-time` command is to stop the process only if it is fatal. A task is defined as fatal if the task gets another watchdog within 12 hours of being assigned the first watchdog, and a handler has been registered.

Examples

The following example shows how to configure the maximum time in milliseconds (to 1000 ms in this example) that a scheduler can run without flagging an error:

```
Router> enable
Router# configure terminal
Router(config)# scheduler max-sched-time 1000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler isr-watchdog</td>
<td>Detects if an ISR is suspended or stalled and manages a watchdog timeout on an ISR.</td>
</tr>
</tbody>
</table>

`scheduler process-watchdog`

To configure the default action of a watchdog timeout for a process using a scheduler, use the `scheduler process-watchdog` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
scheduler process-watchdog {hang|normal|reload|terminate}
no scheduler process-watchdog
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hang</code></td>
<td>Retains the process but does not schedule it.</td>
</tr>
<tr>
<td><code>normal</code></td>
<td>Enables factory-specified per-process behavior.</td>
</tr>
<tr>
<td><code>reload</code></td>
<td>Reloads the system.</td>
</tr>
<tr>
<td><code>terminate</code></td>
<td>Terminates the process and continues.</td>
</tr>
</tbody>
</table>

Command Default

The default value is `normal`.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(1)M.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The watchdog timer sets the interval after which the scheduler assumes a process has been suspended or stalled and needs to be stopped.

Examples

The following example shows how to configure the default action of a watchdog timeout for a process using a scheduler:

```
Router> enable
Router# configure terminal
Router(config)# scheduler process-watchdog normal
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler max-sched-time</td>
<td>Configures the maximum time in milliseconds that a scheduler can run without flagging an error.</td>
</tr>
</tbody>
</table>

scheduler timercheck process

To configure process-level timer validation on a scheduler, and check the timer tree of the process after every context switch of the process Packet Identification number (PID) is configured, use the `scheduler timercheck process` command in global configuration mode. To disable this configuration, use the `no` form of this command.

```
scheduler timercheck process pid
no scheduler timercheck process pid
```

Syntax Description

- `pid` PID number in the range is from 1 to 2147483647.

Command Default

The process-level timer validation is not configured on a scheduler.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(1)M.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify the `show processes timercheck` command after configuring the `scheduler timercheck process` command to display the details of the configuration.

Examples

The following example shows how to configure process-level timer validation on a scheduler with a PID value of 5:

```
Router> enable
Router# configure terminal
Router(config)# scheduler timercheck process 5
Router(config)# show processes timer
System timer check not configured.
Process timer check configuration follows.
PID  Configuration     Name
1    On every context switch. Chunk Manager
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes timercheck</td>
<td>Displays information about the active Cisco IOS processes or the Cisco IOS Software Modularity POSIX-style processes.</td>
</tr>
<tr>
<td>scheduler timercheck system context</td>
<td>Configures system-level validation on context switches on a scheduler.</td>
</tr>
</tbody>
</table>

scheduler timercheck system context

To configure system-level validation on context switches on a scheduler, and check system level-timers, use the **scheduler timercheck system context** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
scheduler timercheck system context
no scheduler timercheck system context
```

**Syntax Description**

This command has no additional keywords or arguments.

**Command Default**

The system-level validation on context switches on a scheduler is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(M)</td>
<td>This command was introduced in a release earlier than Cisco IOS 15.0(M).</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure system level validation on context switches on a scheduler:

```
Router> enable
Router# configure terminal
Router(config)# scheduler timercheck system context
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler timercheck process</td>
<td>Configures process-level timer validation on a scheduler.</td>
</tr>
</tbody>
</table>

send

To send messages to one or all terminal lines, use the `send` command in user or privileged EXEC mode.

```
send {line-number|*|aux number|console number|log number [msg-ext] | tty number|vt y number|xsm
[client client-id] message text
```

**Syntax Description**

- `line-number`
  - Line number to which the message will be sent.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Sends a message to all lines.</td>
</tr>
<tr>
<td>aux number</td>
<td>Sends a message to the specified auxiliary (AUX) port.</td>
</tr>
<tr>
<td>console number</td>
<td>Sends a message to the specified console port.</td>
</tr>
<tr>
<td>log number</td>
<td>Logs a message of the specified severity.</td>
</tr>
<tr>
<td>msg-text</td>
<td>Logging message text.</td>
</tr>
<tr>
<td>client client-id</td>
<td>(Optional) Sends the message to the specified client. The message is sent to all clients if the client ID is not specified.</td>
</tr>
<tr>
<td>message text</td>
<td>Sends a message to XSM client when it is used with the xsm keyword.</td>
</tr>
<tr>
<td>tty number</td>
<td>Sends a message to the specified asynchronous line.</td>
</tr>
<tr>
<td>vty number</td>
<td>Sends a message to the specified virtual asynchronous line.</td>
</tr>
<tr>
<td>xsm client-id</td>
<td>Sends a message to the XML Subscription Manager (XSM) client.</td>
</tr>
</tbody>
</table>

**Command Default**

No messages are sent.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After entering the `send` command, the system prompts for the message to be sent, which can be up to 500 characters long. Press **Ctrl-Z** to end the message. Press **Ctrl-C** to abort this command.

⚠️ **Caution**

Be aware that in some circumstances text sent using the `send` command may be interpreted as an executable command by the receiving device. For example, if the receiving device is UNIX workstation, and the receiving device is in a state (shell) where commands can be executed, the incoming text, if it is a properly formatted UNIX command, will be accepted by the workstation as a command. For this reason, you should limit your exposure to potential messages from terminal servers or other Cisco IOS-based devices when running an interactive shell.
**Examples**

The following example shows how to send a message to all lines:

Router# send
*
Enter message, end with CTRL/Z; abort with CTRL/C:
The system 2509 will be shut down in 10 minutes for repairs.^Z
Send message? [confirm]
Router#
***
*** Message from tty0 to all terminals:
***
The system 2509 will be shut down in 10 minutes for repairs.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reloads the operating system.</td>
</tr>
</tbody>
</table>

**service compress-config**

To compress startup configuration files, use the `service compress-config` command in global configuration mode. To disable compression, use the `no` form of this command.

```
service compress-config
no service compress-config
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you configure the `service compress-config` command, the router will compress configuration files every time you save a configuration to the startup configuration. For example, when you enter the `copy system:running-config nvram:startup-config` command, the running configuration will be compressed before storage in NVRAM.

If the file compression succeeds, the following message is displayed:

```
Compressing configuration from configuration-size
to compressed-size
[OK]
```

If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```
If the file compression fails, the following message is displayed:

Error trying to compress nvram

One way to determine whether a configuration file will be compressed enough to fit into NVRAM is to use a text editor to enter the configuration, then use the UNIX compress command to check the compressed size. To get a closer approximation of the compression ratio, use the UNIX compress -b12 command.

Once the configuration file has been compressed, the router functions normally. At boot time, the system recognizes that the configuration file is compressed, uncompresses it, and proceeds normally. A partition nvram:startup-config command uncompresses the configuration before displaying it.

To disable compression of the configuration file, enter configuration mode and specify the no service compress-config command. Then, exit global configuration mode and enter the copy system:running-config nvram:startup-config command. The router displays an OK message if it is able to write the uncompressed configuration to NVRAM. Otherwise, the router displays an error message indicating that the configuration is too large to store. If the configuration file is larger than the physical NVRAM, the following message is displayed:

##Configuration too large to fit uncompressed in NVRAM Truncate configuration? [confirm]

When the file is truncated, commands at the end of the file are erased. Therefore, you will lose part of your configuration. To truncate and save the configuration, type Y. To not truncate and not save the configuration, type N.

**Examples**

In the following example, the configuration file is compressed:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service compress-config
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# copy system:running-config nvram:startup-config
Building configuration...
Compressing configuration from 1179 bytes to 674 bytes
[OK]
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>partition nvram:startup-config</td>
<td>Separates Flash memory into partitions on Class B file system platforms.</td>
</tr>
</tbody>
</table>

**service config**

To enable autoloading of configuration files from a network server, use the service config command in global configuration mode. To restore the default, use the no form of this command.

```
service config
no service config
```

**Syntax Description**

This command has no arguments or keywords.
Command Default

Autoloading of configuration files from a network server is disabled, except on systems without NVRAM or with invalid or incomplete information in NVRAM. In these cases, autoloading of configuration files from a network server is enabled automatically.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Usually, the service config command is used in conjunction with the boot host or boot network command. You must enter the service config command to enable the router to automatically configure the system from the file specified by the boot host or boot network command. With Cisco IOS software Releases 12.3(2)T, 12.3(1)B, and later releases, you no longer have to specify the service config command for the boot host or boot network command to be active. If you specify both the no service config command and the boot host command, the router attempts to find the specified host configuration file. The service config command can also be used without the boot host or boot network command. If you do not specify host or network configuration filenames, the router uses the default configuration files. The default network configuration file is network-config. The default host configuration file is host-config, where host is the hostname of the router. If the Cisco IOS software cannot resolve its hostname, the default host configuration file is router-config.

Note

You must issue the **reload** command for the **service config** command to take effect.

Examples

In the following example, a router is configured to autoload the default network and host configuration files. Because no **boot host** or **boot network** commands are specified, the router uses the broadcast address to request the files from a TFTP server.

```
Router(config)# service config
```

The following example changes the network configuration filename to bridge_9.1, specifies that rcp is to be used as the transport mechanism, and gives 172.16.1.111 as the IP address of the server on which the network configuration file resides:

```
Router(config)# service config
Router(config)# boot network rcp://172.16.1.111/bridge_9.1
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boot host</strong></td>
<td>Changes the default name of the host configuration filename from which to load configuration commands.</td>
</tr>
<tr>
<td><strong>boot network</strong></td>
<td>Changes the default name of the network configuration file from which to load configuration commands.</td>
</tr>
<tr>
<td><strong>Reload</strong></td>
<td>Reloads the operating system.</td>
</tr>
</tbody>
</table>
**service counters max age**

To set the time interval for retrieving statistics, use the `service counters max age` command in global configuration mode. To return to the default settings, use the `no` form of this command.

```
service counters max age seconds
no service counters max age
```

**Syntax Description**

| `seconds` | Specifies the maximum age in seconds to retrieve statistics from the CLI or SNMP. Valid values are from 0 to 60. |

**Command Default**

By default, `seconds` is 0 seconds.

**Note**

For the 6500 and 7600 platforms, a different value is set at system initialization.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXD</td>
<td>Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.</td>
</tr>
</tbody>
</table>
| 12.2(18)SXF | This command was modified.  
- The default was changed from 10 seconds to 5 seconds.  
- The valid values for `seconds` was changed from 1 to 60 seconds to 0 to 60 seconds. |
| 12.2(33)SRA | This command was integrated in Cisco IOS Release 12.2(33)SRA. |

**Usage Guidelines**

A fully loaded Catalyst 6500 series switch chassis that is running Cisco IOS software version 12.2(18)SXF or its minor variants (SXF through SXF5) takes 1 to 2 minutes to update the SNMP counters maintained under ifTable and ifXTable.

To understand the amount of traffic that a specific port/interface handles, the ifTable/ifXTable is polled. The typical polling interval to meet this is 3 to 5 minutes. There is no advantage if you reduce the polling interval to less than 3 minutes.

**Note**

If you decrease the time interval for retrieving statistics from the default setting (5 seconds), traffic congestion results in situations where frequent SNMP (SNMP bulk) retrievals occur.

**Examples**

This example shows how to set the time interval for retrieving statistics:

```
Router(config)# service counters max age 10
```
This example shows how to return to the default setting:

Router(config)# no service counters max age
Router(config)#

service decimal-tty

To specify that line numbers be displayed and interpreted as octal numbers rather than decimal numbers, use the `no service decimal-tty` command in global configuration mode. To restore the default, use the `service decimal-tty` command.

```
no service decimal-tty
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Enabled (line numbers displayed as decimal numbers)

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the router is configured to display decimal rather than octal line numbers:

```
Router(config)# service decimal-tty
```

service exec-wait

To delay the startup of the EXEC on noisy lines, use the `service exec-wait` command in global configuration mode. To disable the delay function, use the `no` form of this command.

```
no service exec-wait
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command delays startup of the EXEC until the line has been idle (no traffic seen) for 3 seconds. The default is to enable the line immediately on modem activation.

This command is useful on noisy modem lines or when a modem attached to the line is configured to ignore MNP/V.42 negotiations, and MNP/V.42 modems may be dialing in. In these cases, noise or MNP/V.42 packets may be interpreted as usernames and passwords, causing authentication failure before the user has a chance to type a username or password. The command is not useful on nonmodem lines or lines without some kind of login configured.

Examples

The following example delays the startup of the EXEC:

```
Router(config) # service exec-wait
```

grep

The service finger command has been replaced by the ip finger command. However, the service finger and no service finger commands continue to function to maintain backward compatibility with older versions of Cisco IOS software. Support for this command may be removed in a future release. See the description of the ip finger command for more information.

service hide-telnet-address

To hide addresses while trying to establish a Telnet session, use the service hide-telnet-address command in global configuration mode. To disable this service, use the no form of this command.

```
service hide-telnet-address
no service hide-telnet-address
```

Syntax Description

This command has no arguments or keywords.

Command Default

Addresses are displayed.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When you attempt to connect to a device, the router displays addresses and other messages (for example, “Trying router1 (171.69.1.154, 2008)...”). With the hide feature, the router suppresses the display of the address (for example, “Trying router1 address #1...”). The router continues to display all other messages that
would normally be displayed during a connection attempt, such as detailed error messages if the connection was not successful.

The hide feature improves the functionality of the busy-message feature. When you configure only the **busy-message** command, the normal messages generated during a connection attempt are not displayed; only the busy-message is displayed. When you use the hide and busy features together you can customize the information displayed during Telnet connection attempts. When you configure the **service hide-telnet-address** command and the **busy-message** command, the router suppresses the address and displays the message specified with the **busy-message** command if the connection attempt is not successful.

### Examples

The following example hides Telnet addresses:

```
Router(config)# service hide-telnet-address
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>busy-message</strong></td>
<td>Creates a “host failed” message that is displayed when a connection fails.</td>
<td></td>
</tr>
</tbody>
</table>

### service linenum

To configure the Cisco IOS software to display line number information after the EXEC or incoming banner, use the **service linenum** command in global configuration mode. To disable this function, use the **no** form of this command.

```
service linenum
no service linenum
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

Disabled

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

With the **service linenum** command, you can have the Cisco IOS software display the host name, line number, and location each time an EXEC process is started, or an incoming connection is made. The line number banner appears immediately after the EXEC banner or incoming banner. This feature is useful for tracking problems with modems, because the host and line for the modem connection are listed. Modem type information can also be included.

#### Examples

In the following example, a user Telnets to Router2 before and after the **service linenum** command is enabled. The second time, information about the line is displayed after the banner.
Router1> telnet Router2
Trying Router2 (172.30.162.131)... Open
Welcome to Router2.
User Access Verification
Password: Router2>
enable
Password: Router2#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)# service linenumber
Router2(config)# end
Router2# logout
(Connection to Router2 closed by foreign host)
Router1> telnet Router2
Trying Router2 (172.30.162.131)... Open
Welcome to Router2.
Router2 line 10
User Access Verification
Password: Router2>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show users</td>
<td>Displays information about the active lines on the router.</td>
</tr>
</tbody>
</table>

**service nagle**

To enable the Nagle congestion control algorithm, use the `service nagle` command in global configuration mode. To disable the algorithm, use the `no` form of this command.

```plaintext
service nagle
no service nagle
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When using a standard TCP implementation to send keystrokes between machines, TCP tends to send one packet for each keystroke typed. On larger networks, many small packets use up bandwidth and contribute to congestion.

The algorithm developed by John Nagle (RFC 896) helps alleviate the small-packet problem in TCP. In general, it works this way: The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and additional typed characters are saved until the acknowledgment comes back.
The effect is to accumulate characters into larger chunks, and pace them out to the network at a rate matching the round-trip time of the given connection. This method is usually effective for all TCP-based traffic. However, do not use the service nagle command if you have XRemote users on X Window system sessions.

Examples

The following example enables the Nagle algorithm:

```
Router(config)# service nagle
```

```
service prompt config
```

To display the configuration prompt (config), use the service prompt config command in global configuration mode. To remove the configuration prompt, use the no form of this command.

```
no service prompt config
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The configuration prompts appear in all configuration modes.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the no service prompt config command prevents the configuration prompt from being displayed. The prompt is still displayed in EXEC mode. When the service prompt config command is entered, the configuration mode prompt reappears.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no service prompt config
hostname newname
end
newname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
no service prompt config
```

```
newname(config)# service prompt config
```

```
newname(config)# hostname Router
```

```
Router(config)# end
```

```
Router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Specifies or modifies the host name for the network server.</td>
</tr>
<tr>
<td>prompt</td>
<td>Customizes the prompt.</td>
</tr>
</tbody>
</table>
service sequence-numbers

To enable visible sequence numbering of system logging messages, use the service sequence-numbers command in global configuration mode. To disable visible sequence numbering of logging messages, use the no form of this command.

service sequence-numbers
no service sequence-numbers

Syntax Description
This command has no arguments or keywords.

Command Default
Disabled.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Each system status messages logged in the system logging process have a sequence reference number applied. This command makes that number visible by displaying it with the message. The sequence number is displayed as the first part of the system status message. See the description of the logging commands for information on displaying logging messages.

Examples
In the following example logging message sequence numbers are enabled:

.Mar 22 15:28:02 PST: %SYS-5-CONFIG_I: Configured from console by console
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service sequence-numbers
Router(config)# end
Router#
000066: .Mar 22 15:35:57 PST: %SYS-5-CONFIG_I: Configured from console by console

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging on</td>
<td>Enables system logging globally.</td>
</tr>
<tr>
<td>service timestamps</td>
<td>Enables time-stamping of system logging messages or debugging messages.</td>
</tr>
</tbody>
</table>

service slave-log

To allow slave Versatile Interface Processor (VIP) cards to log important error messages to the console, use the service slave-log command in global configuration mode. To disable slave logging, use the no form of this command.
service slave-log
no service slave-log

Syntax Description
This command has no arguments or keywords.

Command Default
This command is enabled by default.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command allows slave slots to log error messages of level 2 or higher (critical, alerts, and emergencies).

Examples
In the following example, the router is configured to log important messages from the slave cards to the console:

Router(config)# service slave-log

The following is sample output generated when this command is enabled:

%IPC-5-SLAVELOG: VIP-SLOT2: IPC-2-NOMEM: No memory available for IPC system initialization

The first line indicates which slot sent the message. The second line contains the error message.

service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the service tcp-keepalives-in command in global configuration mode. To disable the keepalives, use the no form of this command.

service tcp-keepalives-in
no service tcp-keepalives-in

Syntax Description
This command has no arguments or keywords.

Command Default
Disabled

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Examples

In the following example, keepalives on incoming TCP connections are generated:

Router(config)# service tcp-keepalives-in

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service tcp-keepalives-out</td>
<td>Generates keepalive packets on idle outgoing network connections (initiated by a user).</td>
</tr>
</tbody>
</table>

service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the `service tcp-keepalives-out` command in global configuration mode. To disable the keepalives, use the `no` form of this command.

service tcp-keepalives-out
no service tcp-keepalives-out

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples

In the following example, keepalives on outgoing TCP connections are generated:

Router(config)# service tcp-keepalives-out

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service tcp-keepalives-in</td>
<td>Generates keepalive packets on idle incoming network connections (initiated by the remote host).</td>
</tr>
</tbody>
</table>

service tcp-small-servers

To enable small TCP servers such as the Echo, use the `service tcp-small-servers` command in global configuration mode. To disable the TCP server, use the `no` form of this command.
service tcp-small-servers [{max-servers number|no-limit}]  
no service tcp-small-servers [{max-servers number|no-limit}]

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-servers</td>
<td>(Optional) Sets the number of allowable TCP small servers.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Maximum number of TCP small servers. Range is 1 to 2147483647.</td>
</tr>
<tr>
<td>no-limit</td>
<td>(Optional) Allows the number of TCP small servers to have no limit.</td>
</tr>
</tbody>
</table>

### Command Default
TCP small servers are disabled.

### Command Modes
Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
To use the `service tcp-small-servers` command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your Authentication, Authorization, and Accounting (AAA) administrator for assistance.

The TCP small servers consist of three services: Discard (port 9), Echo (port 7), and Chargen (port 19). These services are used to test the TCP transport functionality. The discard server receives data and discards it. The echo server receives data and echoes the same data to the sending host. The chargen server generates a sequence of data and sends it to the remote host.

### Examples

The following example shows how to enable small TCP servers and set the maximum number of allowable small servers to 14:

```
Router(config)#
  service tcp-small-servers max-servers 14
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service udp-small-servers</td>
<td>Enables small UDP servers such as the Echo.</td>
</tr>
</tbody>
</table>
**service telnet-zeroidle**

To set the TCP window to zero (0) when the Telnet connection is idle, use the `service telnet-zeroidle` command in global configuration mode. To disable this service, use the `no` form of this command.

```
service telnet-zero-idle
no service telnet-zero-idle
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The TCP window is not set to zero when the Telnet connection is idle.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Normally, data sent to noncurrent Telnet connections is accepted and discarded. When the `service telnet-zero-idle` command is enabled, if a session is suspended (that is, some other connection is made active or the router is in the privileged EXEC mode), the TCP window is set to zero. This action prevents the remote host from sending any more data until the connection is resumed. Use this command when it is important that all messages sent by the host be seen by the users and the users are likely to use multiple sessions.

Do not use this command if your host will eventually time out and log out a TCP user whose window is zero.

**Examples**

The following example shows how to set the TCP window to zero when the Telnet connection is idle:

```
Router(config)# service telnet-zeroidle
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>resume</code></td>
<td>Switches to another open Telnet, rlogin, LAT, or PAD session.</td>
</tr>
</tbody>
</table>

**service timestamps**

To configure the system to apply a time stamp to debugging messages or system logging messages, use the `service timestamps` command in global configuration mode. To disable this service, use the `no` form of this command.

```
service timestamps [{debug|log}] [{uptime|datetime [msec]}] [localtime] [show-timezone] [year]
no service timestamps [{debug|log]}
```
## Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug</strong></td>
<td>(Optional) Indicates time-stamping for debugging messages.</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>(Optional) Indicates time-stamping for system logging messages.</td>
</tr>
<tr>
<td><strong>uptime</strong></td>
<td>(Optional) Specifies that the time stamp should consist of the time since the system was last rebooted. For example “4w6d” (time since last reboot is 4 weeks and 6 days).</td>
</tr>
<tr>
<td></td>
<td>• This is the default time-stamp format for both debugging messages and logging messages.</td>
</tr>
<tr>
<td></td>
<td>• The format for uptime varies depending on how much time has elapsed:</td>
</tr>
<tr>
<td></td>
<td>• $HHHH:MM:SS$ ($HHHH$ hours: $MM$ minutes: $SS$ seconds) for the first 24 hours</td>
</tr>
<tr>
<td></td>
<td>• $D , dHH$ $h$ ($D$ days $HH$ hours) after the first day</td>
</tr>
<tr>
<td></td>
<td>• $W , wD , d$ ($W$ weeks $D$ days) after the first week</td>
</tr>
<tr>
<td><strong>datetime</strong></td>
<td>(Optional) Specifies that the time stamp should consist of the date and time.</td>
</tr>
<tr>
<td></td>
<td>• The time-stamp format for datetime is $MMM , DD:HH:MM:SS$, where $MMM$ is the month, $DD$ is the date, $HH$ is the hour (in 24-hour notation), $MM$ is the minute, and $SS$ is the second.</td>
</tr>
<tr>
<td></td>
<td>• If the datetime keyword is specified, you can optionally add the msec localtime, show-timezone, or year keywords.</td>
</tr>
<tr>
<td></td>
<td>• If the service timestamps datetime command is used without additional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.</td>
</tr>
<tr>
<td><strong>msec</strong></td>
<td>(Optional) Includes milliseconds in the time stamp, in the format $HH:DD:MM:SS.mmm$, where .$mmm$ is milliseconds</td>
</tr>
<tr>
<td><strong>localtime</strong></td>
<td>(Optional) Time stamp relative to the local time zone.</td>
</tr>
<tr>
<td><strong>year</strong></td>
<td>(Optional) Include the year in the date-time format.</td>
</tr>
<tr>
<td><strong>show-timezone</strong></td>
<td>(Optional) Include the time zone name in the time stamp.</td>
</tr>
</tbody>
</table>

### Note

If the localtime keyword option is not used (or if the local time zone has not been configured using the clock timezone command), time will be displayed in Coordinated Universal Time (UTC).

## Command Default

Time stamps are applied to debug and logging messages.

## Command Modes

Global configuration (config)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(5)</td>
<td>Service time stamps are enabled by default.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>The year keyword was added.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

Time stamps can be added to either debugging messages (`service timestamp debug`) or logging messages (`service timestamp log`) independently.

If the `service timestamps` command is specified with no arguments or keywords, the default is `service timestamps debug uptime`.

The `no service timestamps` command by itself disables time stamps for both debug and log messages.

The `uptime` form of the command adds time stamps (such as “2w3d”) that indicating the time since the system was rebooted. The `datetime` form of the command adds time stamps (such as “Sep 5 2002 07:28:20”) that indicate the date and time according to the system clock.

Entering the `service timestamps {debug | log} command a second time will overwrite any previously configured `service timestamp {debug | log} commands and associated options.`

To set the local timezone, use the `clock timezone zone hours-offset` command in global configuration mode.

The time stamp will be preceded by an asterisk or period if the time is potentially inaccurate. The table below describes the symbols that precede the time stamp.

#### Table 42: Time-Stamping Symbols for syslog Messages

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>(blank)</td>
<td>Time is authoritative: the software clock is in sync or has just been set manually</td>
<td>15:29:03.158 UTC Tue Feb 25 2003:</td>
</tr>
<tr>
<td>*</td>
<td>Time is not authoritative: the software clock has not been set, or is not in sync with configured Network Time Protocol (NTP) servers.</td>
<td>*15:29:03.158 UTC Tue Feb 25 2003:</td>
</tr>
<tr>
<td>.</td>
<td>Time is authoritative, but the NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.</td>
<td>.15:29:03.158 UTC Tue Feb 25 2003:</td>
</tr>
</tbody>
</table>

### Examples

In the following example, the router begins with time-stamping disabled. Then, the default time-stamping is enabled (uptime time stamps applied to debug output). Then, the default time-stamping for logging is enabled (uptime time stamps applied to logging output).

```
Router# show running-config | include time

no service timestamps debug uptime
no service timestamps log uptime
Router# config terminal
```
Router(config)# service timestamps

! issue the show running-config command in config mode using do
show running-config | inc time

! shows that debug timestamping is enabled, log timestamping is disabled
service timestamps debug uptime
no service timestamps log uptime
! enable timestamps for logging messages
Router(config)# service timestamps log
Router(config)# do show run | inc time

service timestamps debug uptime
service timestamps log uptime
Router(config)# service sequence-numbers

Router(config)# end

000075: 5w0d: %SYS-5-CONFIG_I: Configured from console by console
! The following is a level 5 system logging message
! The leading number comes from the service sequence-numbers command.
! 4w6d indicates the timestamp of 4 weeks, 6 days000075: 4w6d: %SYS-5-CONFIG_I: Configured from console by console

In the following example, the user enables time-stamping on logging messages using the current time and date in Coordinated Universal Time/Greenwich Mean Time (UTC/GMT), and enables the year to be shown.

Router(config)#

! The following line shows the timestamp with uptime (1 week 0 days)
1w0d: %SYS-5-CONFIG_I: Configured from console by console
Router(config)# service timestamps log datetime show-timezone year

Router(config)# end

! The following line shows the timestamp with datetime (11:13 PM March 22nd)
Mar 22 2004 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console

The following example shows the change from UTC to local time:

Router# configure terminal

! Logging output can be quite long; first changing line width to show full
! logging message
Router(config)# line 0

Router(config-line)# width 180

Router(config-line)# logging synchronous

Router(config-line)# end

! Timestamping already enabled for logging messages; time shown in UTC.
Oct 13 23:20:05 UTC: %SYS-5-CONFIG_I: Configured from console by console
Router# show clock

Router# configure terminal

Enter configuration commands, one per line. End with the end command.
! Timezone set as Pacific Standard Time, with an 8 hour offset from UTC
Router(config)# clock timezone PST -8
Router(config)#
Oct 13 23:21:27 UTC: %SYS-6-CLOCKUPDATE:
    System clock has been updated from 23:21:27 UTC Wed Oct 13 2004
Router(config)#
! Pacific Daylight Time (PDT) configured to start in April and end in October.
! Default offset is +1 hour.
Router(config)# clock summer-time PDT recurring first Sunday April 2:00 last Sunday October 2:00
Router(config)#
! Time changed from 3:22 P.M. Pacific Standard Time (15:22 PST)
! to 4:22 P.M. Pacific Daylight (16:22 PDT)

Oct 13 23:22:09 UTC: %SYS-6-CLOCKUPDATE:
    System clock has been updated from 15:22:09 PST Wed Oct 13 2004
    ! Change the timestamp to show the local time and timezone.
Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# end

Oct 13 16:23:19 PDT: %SYS-5-CONFIG_I: Configured from console by console
Router# show clock
Router# config t
Enter configuration commands, one per line. End with the end command.
Router(config)# service sequence-numbers
Router(config)# end

Router#

In the following example, the service timestamps log datetime command is used to change previously configured options for the date-time time stamp.

Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# end
! The year is not displayed.
Oct 13 15:44:46 PDT: %SYS-5-CONFIG_I: Configured from console by console
Router# config t
Enter configuration commands, one per line. End with the end command.
Router(config)# service timestamps log datetime show-timezone year
Router(config)# end

! note: because the
    localtime option was not specified again, that option is
! removed from the output, and time is displayed in UTC (the default)

Oct 13 2004 22:45:31 UTC: %SYS-5-CONFIG_I: Configured from console by console

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock set</td>
<td>Manually sets the system clock.</td>
</tr>
</tbody>
</table>
service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the Echo, use the `service udp-small-servers` command in global configuration mode. To disable the UDP server, use the `no` form of this command.

```plaintext
service udp-small-servers [{max-servers number|no-limit}]
no service udp-small-servers [{max-servers number|no-limit}]
```

**Syntax Description**

- `max-servers` (Optional) Sets the number of allowable UDP small servers.
- `number` (Optional) Maximum number of UDP small servers. Range is 1 to 2147483647.
- `no-limit` (Optional) Allows the number of TCP small servers to have no limit.

**Command Default**

UDP small servers are disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your Authentication, Authorization, and Accounting (AAA) administrator for assistance.

The UDP small servers currently consist of three services: Discard (port 9), Echo (port 7), and Chargen (port 19). These services are used to test the UDP transport functionality. The discard server receives data and discards it. The echo server receives data and echoes the same data to the sending host. The chargen server generates a sequence of data and sends it to the remote host.

**Examples**

The following example shows how to enable small UDP servers and set the maximum number of allowable small servers to 10:
service-module apa traffic-management

To configure traffic management on the router, use the `service-module apa traffic-management` command in interface configuration mode.

```
service-module apa traffic-management [{monitor|inline}]`
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Enables promiscuous monitoring.</td>
</tr>
<tr>
<td>inline</td>
<td>Enables inline monitoring.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

Interface configuration mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)YA</td>
<td>This command was introduced for the NME-APA on Cisco 2811, 2821, 2851, and Cisco 3800 Series Integrated Services Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To perform traffic management, you enable or disable the flow of packets by configuring the service module interface and the router interface.

- Configure the router interface with the `service-module apa traffic-management [monitor | inline]` command.

Two traffic management options are available:

- Monitor--will copy the packet and designate the copy as the one forwarded to the Application Performance Assurance module (NME-APA).
- Inline--will send the packet to the NME-APA, rather than sending a copy of the packet. After the NME-APA has processes the packet, it sends it back to the router.

Note

Enable only one traffic management option on the router, but not both concurrently.

- Configure the service module interface with the Application Performance Assurance (APA) graphical user interface (GUI). See the Cisco Application Performance Assurance User Guide for details.
Examples

The following example configures an interface on a Cisco 2851 Integrated Services Router for inline traffic management.

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ip address 10.10.43.255.255.255.0
Router(config-if)# service-module apa traffic-management inline
Router(config-if)# exit
end
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface gigabitethernet</td>
<td>Defines the interface on the router</td>
</tr>
<tr>
<td>ip address</td>
<td>Defines the IP address and subnet mask on the interface</td>
</tr>
</tbody>
</table>

**service-module wlan-ap bootimage**

To configure the boot image on the service module, use the `service-module wlan-ap bootimage` command in privileged EXEC mode.

```
service-module wlan-ap interface number bootimage [{autonomous|unified}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>interface number</th>
<th>The interface number for the wireless device. Always use 0.</th>
</tr>
</thead>
<tbody>
<tr>
<td>autonomous</td>
<td>Autonomous software image.</td>
</tr>
<tr>
<td>unified</td>
<td>Upgrade image with Lightweight Access Point Protocol (LWAPP).</td>
</tr>
</tbody>
</table>

**Command Default**

Autonomous software image

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20) T</td>
<td>This command was introduced for wireless-enabled Cisco 880 Series and Cisco 890 Series Integrated Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When running the advanced IP services feature set on either Cisco 880 Series routers or Cisco 890 Series routers, use the `service-module wlan-ap 0 bootimage unified command` to enable the Cisco unified software upgrade image on the embedded wireless access point. After enabling the unified image, use the `service-module wlan-ap 0 reload` command to perform a graceful shutdown and reboot of the access point.

**Note**

The `service-module wlan-ap 0 bootimage` command does not support recovery images on the embedded access point. Use the `service-module wlan-ap 0 reload` command to shutdown and reboot the access point.
Cisco 880 Series and Cisco 890 Series routers with embedded access point running the unified software image require DHCP to obtain an IP address for the access point. An IP address is needed to communicate with the Wireless LAN Controller (WLC) and to download its image upon boot up. The host router can provide DHCP server functionality through the DHCP pool to reach the WLC, and setup option 43 for the controller IP address in the DHCP pool configuration.

Use the following guideline to setup a DHCP pool on the host router.

```
ip dhcp pool embedded-ap-pool
  network 60.0.0.0 255.255.255.0
  default router 60.0.0.1
  option 43 hex f104.0a0a.0a0f /* Single WLC IP address (10.10.10.15) in HEX format */
  int vlan 1 /* Default Vlan */
ip address 60.0.0.1 255.255.255.0
int Wlan-GigabitEthernet0 /* internal switch-port to AP */
switchport access vlan 1
```

Examples

The following example upgrades the embedded access point image from autonomous to unified.

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage unified
*Jan 18 05:31:58.172: %WLAN_AP_SM-6-UNIFIED_IMAGE: Embedded AP will change boot image to mini-IOS also called LWAPP recovery Please check router config to ensure connectivity between WLC and AP. Use service-module wlan-ap 0 reload to bootup mini-IOS image on AP
Router(config)# end
Router# service-module wlan-ap 0 reload
Reload will save AP config...
Do you want to proceed with reload?[confirm] Trying to reload Service Module wlan-ap0.
Router# Service Module saved config, start reset.
Received reload request from router
Saving configuration...
Building configuration...
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface wlan-ap</td>
<td>Enters wireless interface configuration mode to configure an interface.</td>
</tr>
<tr>
<td></td>
<td>service-module wlan-ap reload</td>
<td>Performs a graceful shutdown and reboot of the service module.</td>
</tr>
<tr>
<td></td>
<td>service-module wlan-ap reset</td>
<td>Resets the service module hardware.</td>
</tr>
</tbody>
</table>

**service-module wlan-ap reload**

To perform a graceful shutdown and reboot of the service module use the `service-module wlan-ap reload` command in privileged EXEC mode.

```
service-module wlan-ap interface number reload
```

| Syntax Description | interface number | The interface number for the wireless device. Always use 0. |
Command Default
None

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Autonomous Mode
At the confirmation prompt, press Enter to confirm the action, or press n to cancel.

Note
When running in autonomous mode, the reload command saves the configuration before rebooting. If the attempt is unsuccessful, the following message displays: Failed to save service module configuration.

Unified Mode
The service module reload command is usually handled by the Wireless LAN Controller (WLC).

Note
When running in Unified mode, the reload command will produce the following message: The embedded wireless device is in Unified mode. Reload/reset is normally handled by WLC controller. Still want to proceed? [yes]

Examples

The following examples show a graceful shut down and reboot of the service module:

Autonomous Mode

Router# service-module wlan-ap0 reload
Do you want to proceed with reload?[confirm]
Router# reload
Do you want to reload the internal AP? [yes/no]:
Do you want to save the configuration of the AP? [yes/no]:
System configuration has been modified. Save [yes/no]:
Proceed with reload? [confirm]

Unified Mode

Router# service-module wlan-ap0 reload
The embedded AP is in Unified mode. Reload/reset is normally handled by WLC controller. Still want to proceed? [yes]
Router# reload
The embedded AP is in Unified mode. Reload/reset is normally handled by WLC controller.
Do you want to reload the internal AP [yes/no]:
System configuration has been modified. Save [yes/no]:
Proceed with reload [Confirm]
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface wlan-ap</td>
<td>Enters wireless interface configuration mode to configure an interface.</td>
</tr>
<tr>
<td>service-module wlan-ap reset</td>
<td>Resets the service module hardware.</td>
</tr>
</tbody>
</table>

**service-module wlan-ap reset**

To reset the service module hardware, software, and configuration, use the `service-module wlan-ap reset` command in privileged EXEC mode.

```
service-module wlan-ap interface number reset [{bootloader|default-config}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface number</td>
<td>The interface number for the wireless device. Always use 0.</td>
</tr>
<tr>
<td>bootloader</td>
<td>Resets the wireless device to the bootloader for manual image recovery.</td>
</tr>
<tr>
<td>default-config</td>
<td>Resets the wireless device to the factory default configuration.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

At the confirmation prompt, press Enter to confirm the action, or press n to cancel.

⚠️ **Caution**

Because you may lose data, use the `service-module wlan-ap reset` command only to recover from a shutdown or failed state.

**Examples**

The following example resets a wireless device on a router that is operating in either autonomous mode or LWAPP mode:

**Autonomous Mode**

```
Router# service-module wlan-ap0 reset
Use reset only to recover from shutdown or failed state.
```

**LWAPP Mode**

```
Router# service-module wlan-ap0 reset
```
The embedded device is in LWAPP mode. Reload/reset is normally handled by WLC controller. Still want to proceed? [yes]

**Resetting the Factory Default Configuration on the Wireless Device**

The following example resets the wireless device to the default configuration.

Router#service-module wlan-ap 0 reset default-config
Router#

**Recovering the Image on the Wireless Device**

The following example resets the wireless device down to the bootloader level for manual image recovery.

Router#service-module wlan-ap0 reset bootloader
Router#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface wlan-ap</code></td>
<td>Enters wireless interface configuration mode to configure an interface.</td>
</tr>
<tr>
<td><code>service-module wlan-ap reload</code></td>
<td>Performs a graceful shutdown and reboot of the service module.</td>
</tr>
</tbody>
</table>

### service-module wlan-ap session

To begin a configuration session with a service module through a console connection use the `service-module wlan-ap session` command in privileged EXEC mode.

```
service-module wlan-ap interface number session [{clear|disconnect}]
```

#### Syntax Description

<table>
<thead>
<tr>
<th><strong>interface number</strong></th>
<th>The interface number for the wireless device. Always use 0.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear</strong></td>
<td>(Optional) Clears the wireless device configuration session.</td>
</tr>
</tbody>
</table>

#### Command Default

None

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Only one session is allowed at a time into the wireless device from a router console-port connection. After starting a session, perform configuration tasks on the wireless device. You first access the router in a user-level
To access the privileged EXEC command shell, where most commands are available, use the `enable` command.

When you finish configuring the device, and would like to exit the console session, type Ctrl-Shift 6x to return to the router’s console. Type service-module wlan-ap session `clear` or disconnect to close the session with the device. At the confirmation prompt, press `Enter twice` to confirm the action or `n` to cancel.

**Note**

If you do not clear or disconnect the session on the service module, it will remain open in the background after you return to the router's console prompt. When the session is open in the background, pressing Enter will toggle you back to the wireless device prompt.

**Examples**

The following example shows a session being opened on a service-module in an ISR:

```
Router# service-module wlan-ap 0 session
Trying 1.2.3.4, 2002 ... Open
AP#
```

The following example clears the session on the service-module in the ISR:

```
Router# service-module wlan-ap 0 session clear
[confirm]
[OK]
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><code>interface wlan-ap</code></td>
<td>Enters wireless interface configuration mode to configure an interface.</td>
</tr>
</tbody>
</table>

**service-module wlan-ap statistics**

To display reset and reload information for a service module and its operating system software, use the `service-module wlan-ap statistics` command in privileged EXEC mode.

```
service-module wlan-ap statistics
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>interface number</strong></th>
<th>The interface number for the wireless device. Always use 0.</th>
</tr>
</thead>
</table>

**Command Default**

none

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.</td>
</tr>
</tbody>
</table>
The following example displays information for wireless-enabled Cisco ISRs:

```
Router#service-module wlan-ap 0 statistics
Module Reset Statistics:
    CLI reset count = 0
    CLI reload count = 1
    Registration request timeout reset count = 0
    Error recovery timeout reset count = 0
    Module registration count = 10
The last IOS initiated event was a cli reload at *04:27:32.041 UTC Fri Mar 8 2007
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface wlan-ap</code></td>
<td>Enters wireless interface configuration mode and configures a wireless device.</td>
</tr>
<tr>
<td><code>service-module wlan-ap reset</code></td>
<td>Resets the wireless device.</td>
</tr>
<tr>
<td><code>service-module wlan-ap reload</code></td>
<td>Performs a graceful shutdown and reboot on the wireless device.</td>
</tr>
</tbody>
</table>

### service-module wlan-ap status

To display configuration information related to hardware and software on the service module, use the `service-module wlan-ap status` command in privileged EXEC mode.

```
service-module wlan-ap interface number status
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>interface number</code></th>
<th>The interface number for the wireless device. Always use 0.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Display the wireless device’s software release version
- Check the wireless device’s status (steady or down)
- Display hardware information for the wireless device, including image, memory, interface, and system uptime

**Examples**

The following example displays information for the wireless device on a Cisco Integrated Services Router:
Router# service-module wlan-ap 0 status

Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..
Image path = flash:c8xx_19xx_ap-k9w7=m.x.acregr/c8xx_19xx_ap-k9w7=m.x.acregr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Cisco 860 and 880 Series Integrated Services Routers.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface wlan-ap</td>
<td>Enters wireless service module's console interface.</td>
</tr>
</tbody>
</table>

**session slot**

To open a session with a module (for example, the Multilayer Switch Module (MSM), Network Analysis Module (NAM), or Asynchronous Transfer Mode (ATM)), use the `session slot` command in EXEC mode.

```
Router# session slot mod processor processor-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>mod</th>
<th>Slot number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>processor processor-id</td>
<td>Specifies the processor ID.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To end the session, enter the `quit` command.

This command allows you to use the module-specific CLI.

**Examples**

This example shows how to open a session with an MSM (module 4):

```
Router# session slot 4 processor 2
Router#
```
set memory debug incremental starting-time

To set the current time as the starting time for incremental analysis, use the `set memory debug incremental starting-time` command in privileged EXEC mode.

```
set memory debug incremental starting-time [none]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>(Optional) Resets the defined start time for incremental analysis.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For incremental analysis, a starting point can be defined by using the `set memory debug incremental starting-time` command. When a starting time is set, only memory allocated after that starting time will be considered for reporting as leaks.

**Examples**

The following example shows the command used to set the starting time for incremental analysis to the time when the command was issued:

```
Router# set memory debug incremental starting-time
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory debug incremental allocation</td>
<td>Displays all memory blocks that were allocated after the issue of the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td>show memory debug incremental leaks</td>
<td>Displays only memory that was leaked after the issue of the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td>show memory debug incremental leaks lowmem</td>
<td>Forces incremental memory leak detection to work in low memory mode. Displays only memory that was leaked after the issue of the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td>show memory debug incremental status</td>
<td>Displays if the starting point of incremental analysis has been defined and the time elapsed since then.</td>
</tr>
<tr>
<td>show memory debug leaks</td>
<td>Displays detected memory leaks.</td>
</tr>
</tbody>
</table>
setup

To enter Setup mode, use the `setup` command in privileged EXEC mode.

**setup**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Setup mode gives you the option of configuring your system without using the Cisco IOS Command Line Interface (CLI). For some tasks, you may find it easier to use Setup than to enter Cisco IOS commands individually. For example, you might want to use Setup to add a protocol suite, to make major addressing scheme changes, or to configure a newly installed interface. Although you can use the CLI to make these changes, Setup provides you with a high-level view of the configuration and guides you through the configuration process.

If you are not familiar with Cisco products and the CLI, Setup is a particularly valuable tool because it prompts you for the specific information required to configure your system.

**Note**

If you use the Setup mode to modify a configuration because you have added or modified the hardware, be sure to verify the physical connections using the `show version` EXEC command. Also, verify the logical port assignments using the `show running-config` EXEC command to ensure that you configure the correct port. Refer to the hardware documentation for your platform for more information on physical and logical port assignments.

Before using the Setup mode, you should have the following information so that you can configure the system properly:

- Which interfaces you want to configure
- Which routing protocols you wish to enable
- Whether the router is to perform bridging
- Network addresses for the protocols being configured
- Password strategy for your environment

When you enter the `setup` EXEC command after first-time startup, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. It prompts you first for global parameters and then for interface parameters. The values shown in brackets next to each prompt reflect either the default settings or the last configured setting.
The prompts and the order in which they appear on the screen vary depending on the platform and the interfaces installed in the device.

You must progress through the System Configuration Dialog until you come to the item that you intend to change. To accept default settings for items that you do not want to change, press the Return or Enter key. The default choice is indicated by square brackets (for example, [yes]) before the prompt colon (:).

To exit Setup mode and return to privileged EXEC mode without making changes and without progressing through the entire System Configuration Dialog, press Ctrl-C.

The facility also provides help text for each prompt. To access help text, press the question mark (?) key at a prompt.

When you complete your changes, the system will automatically display the configuration file that was created during the Setup session. It also asks you if you want to use this configuration. If you answer Yes, the configuration is saved to NVRAM as the startup configuration file. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

**Examples**

The following example displays the setup command facility to configure serial interface 0 and to add ARAP and IP/IPX PPP support on the asynchronous interfaces:

```bash
Router# setup
--- System Configuration Dialog
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[ ]'.
First, would you like to see the current interface summary? [yes]:
Interface IP-Address OK? Method Status Protocol
Ethernet0 172.16.72.2 YES manual up up
Serial0 unassigned YES not set administratively down down
Serial1 172.16.72.2 YES not set administratively down down
Configuring global parameters:
Enter host name [Router]:
The enable secret is a one-way cryptographic secret used instead of the enable password when it exists.
Enter enable secret [Use current secret]:
The enable password is used when there is no enable secret and when using older software and some boot images.
Enter enable password [ww]: Enter virtual terminal password [ww]:
Configure SNMP Network Management? [yes]:
   Community string [public]:
Configure DECnet? [no]:
Configure AppleTalk? [yes]:
   Multizone networks? [no]: yes
Configure IPX? [yes]:
Configure IP? [yes]:
   Configure IGRP routing? [yes]:
      Your IGRP autonomous system number [15]:
   Configure Async lines? [yes]:
      Async line speed [9600]: 57600
   Configure for HW flow control? [yes]:
   Configure for modems? [yes/no]: yes
```

Cisco IOS Configuration Fundamentals Command Reference
Configure for default chat script? [yes]: no
Configure for Dial-in IP SLIP/PPP access? [no]: yes
Configure for Dynamic IP addresses? [yes]: no
Configure Default IP addresses? [no]: yes
Configure for TCP Header Compression? [yes]: no
Configure for routing updates on async links? [no]:
Configure for Async IPX? [yes]:
Configure for AppleTalk Remote Access? [yes]:
AppleTalk Network for ARAP clients [1]: 20
Zone name for ARAP clients [ARA Dialins]:

Configuring interface parameters:
Configuring interface Ethernet0:
Is this interface in use? [yes]:
Configure IP on this interface? [yes]:
IP address for this interface [172.16.72.2]:
Class B network is 172.16.0.0, 8 subnet bits; mask is /24
Configure AppleTalk on this interface? [yes]:
Extended AppleTalk network? [yes]:
AppleTalk starting cable range [1]:
AppleTalk ending cable range [1]:
AppleTalk zone name [Sales]:
AppleTalk additional zone name:
Configure IPX on this interface? [yes]:
IPX network number [1]:

Configuring interface Serial0:
Is this interface in use? [no]: yes
Configure IP on this interface? [no]: yes
Assign to which interface [Ethernet0]:
Configure AppleTalk on this interface? [no]: yes
Extended AppleTalk network? [yes]:
AppleTalk starting cable range [2]: 3
AppleTalk ending cable range [3]: 3
AppleTalk zone name [myzone]: ZZ Serial
AppleTalk additional zone name:
Configure IPX on this interface? [no]: yes
IPX network number [2]: 3

Configuring interface Serial1:
Is this interface in use? [yes]:
Configure IP on this interface? [yes]:
Assign to which interface [Ethernet0]:
Configure AppleTalk on this interface? [yes]:
Extended AppleTalk network? [yes]:
AppleTalk starting cable range [2]:
AppleTalk ending cable range [2]:
AppleTalk zone name [ZZ Serial]:
AppleTalk additional zone name:
Configure IPX on this interface? [yes]:
IPX network number [2]:

Configuring interface Async1:
IPX network number [4]:
Default client IP address for this interface [none]: 172.16.72.4

Configuring interface Async2:
IPX network number [5]:
Default client IP address for this interface [172.16.72.5]:

Configuring interface Async3:
IPX network number [6]:
Default client IP address for this interface [172.16.72.6]:

Configuring interface Async4:
IPX network number [7]:
Default client IP address for this interface [172.16.72.7]:
Configuring interface Async5:
  IPX network number [8]:
  Default client IP address for this interface [172.16.72.8]:
Configuring interface Async6:
  IPX network number [9]:
  Default client IP address for this interface [172.16.72.9]:
Configuring interface Async7:
  IPX network number [A]:
  Default client IP address for this interface [172.16.72.10]:
Configuring interface Async8:
  IPX network number [B]:
  Default client IP address for this interface [172.16.72.11]:
Configuring interface Async9:
  IPX network number [C]:
  Default client IP address for this interface [172.16.72.12]:
Configuring interface Async10:
  IPX network number [D]:
  Default client IP address for this interface [172.16.72.13]:
Configuring interface Async11:
  IPX network number [E]:
  Default client IP address for this interface [172.16.72.14]:
Configuring interface Async12:
  IPX network number [F]:
  Default client IP address for this interface [172.16.72.15]:
Configuring interface Async13:
  IPX network number [10]:
  Default client IP address for this interface [172.16.72.16]:
Configuring interface Async14:
  IPX network number [11]:
  Default client IP address for this interface [172.16.72.17]:
Configuring interface Async15:
  IPX network number [12]:
  Default client IP address for this interface [172.16.72.18]:
Configuring interface Async16:
  IPX network number [13]:
  Default client IP address for this interface [172.16.72.19]:
The following configuration command script was created:
hostname Router
enable secret 5 $1$krIg$emfYm/1OwHVspDuS8Gy0K1
enable password ww
line vty 0 4
password ww
snmp-server community public
   !
no decnet routing
appletalk routing
ipx routing
ip routing
   !
line 1 16
speed 57600
flowcontrol hardware
modem inout
   !
arap network 20 ARA Dialins
line 1 16
arap enable
autoselect
   !
! Turn off IPX to prevent network conflicts.
interface Ethernet0
no ipx network
interface Serial0
no ipx network
interface Serial1
no ip x network
!
interface Ethernet0
ip address 172.16.72.2 255.255.255.0
appletalk cable-range 1-1 1.204
appletalk zone Sales
ip x network 1
no mop enabled
!
interface Serial0
no shutdown
no ip address
ip unnumbered Ethernet0
appletalk cable-range 3-3
appletalk zone ZZ Serial
ip x network 3
no mop enabled
!
interface Serial1
no ip address
ip unnumbered Ethernet0
appletalk cable-range 2-2 2.2
appletalk zone ZZ Serial
ip x network 2
no mop enabled
!
interface Async1
ip x network 4
ip unnumbered Ethernet0
peer default ip address 172.16.72.4
async mode interactive
!
interface Async2
ip x network 5
ip unnumbered Ethernet0
peer default ip address 172.16.72.5
async mode interactive
!
interface Async3
ip x network 6
ip unnumbered Ethernet0
peer default ip address 172.16.72.6
async mode interactive
!
interface Async4
ip x network 7
ip unnumbered Ethernet0
peer default ip address 172.16.72.7
async mode interactive
async dynamic address
!
interface Async5
ip x network 8
ip unnumbered Ethernet0
peer default ip address 172.16.72.8
async mode interactive
!
interface Async6
ip x network 9
ip unnumbered Ethernet0
peer default ip address 172.16.72.9
async mode interactive
!
Interface Async7
ipx network A
ip unnumbered Ethernet0
peer default ip address 172.16.72.10
async mode interactive
!
Interface Async8
ipx network B
ip unnumbered Ethernet0
peer default ip address 172.16.72.11
async mode interactive
!
Interface Async9
ipx network C
ip unnumbered Ethernet0
peer default ip address 172.16.72.12
async mode interactive
!
Interface Async10
ipx network D
ip unnumbered Ethernet0
peer default ip address 172.16.72.13
async mode interactive
!
Interface Async11
ipx network E
ip unnumbered Ethernet0
peer default ip address 172.16.72.14
async mode interactive
!
Interface Async12
ipx network F
ip unnumbered Ethernet0
peer default ip address 172.16.72.15
async mode interactive
!
Interface Async13
ipx network 10
ip unnumbered Ethernet0
peer default ip address 172.16.72.16
async mode interactive
!
Interface Async14
ipx network 11
ip unnumbered Ethernet0
peer default ip address 172.16.72.17
async mode interactive
!
Interface Async15
ipx network 12
ip unnumbered Ethernet0
peer default ip address 172.16.72.18
async mode interactive
!
Interface Async16
ipx network 13
ip unnumbered Ethernet0
peer default ip address 172.16.72.19
async mode interactive
!
router igrp 15
network 172.16.0.0
!
end
Use this configuration? [yes/no]: **yes**
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Router#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>erase nvram:</strong></td>
<td>Erases a file system.</td>
</tr>
<tr>
<td><strong>show running-config</strong></td>
<td>Displays the running configuration file. Command alias for the <code>more</code></td>
</tr>
<tr>
<td></td>
<td><code>system:running-config</code> command.</td>
</tr>
<tr>
<td><strong>show startup-config</strong></td>
<td>Displays the startup configuration file. Command alias for the <code>more</code></td>
</tr>
<tr>
<td></td>
<td><code>system:startup-config</code> command.</td>
</tr>
<tr>
<td><strong>show version</strong></td>
<td>Displays the configuration of the system hardware, the software version, the</td>
</tr>
<tr>
<td></td>
<td>names and sources of configuration files, and the boot images.</td>
</tr>
</tbody>
</table>
show through show fm summary

- show through show fm summary, on page 492
show through show fm summary

show

To verify the Multiple Spanning Tree (MST) configuration, use the `show` command in MST configuration mode.

```
show [{current|pending}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>current</code></td>
<td>(Optional) Displays the current configuration that is used to run MST.</td>
</tr>
<tr>
<td><code>pending</code></td>
<td>(Optional) Displays the edited configuration that will replace the current configuration.</td>
</tr>
</tbody>
</table>

### Command Default

This command has no default settings.

### Command Modes

MST configuration (config-mst)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The display output from the `show pending` command is the edited configuration that will replace the current configuration if you enter the `exit` command to exit MST configuration mode.

Entering the `show` command with no arguments displays the pending configurations.

### Examples

This example shows how to display the edited configuration:

```
Router(config-mst)# show pending
Pending MST configuration
Name     [zorglub]
Version  31415
Instance  Vlans Mapped
---------- ---------------------------------------------------------------
0  4001-4096
2  1010, 1020, 1030, 1040, 1050, 1060, 1070, 1080, 1090, 1100, 1110
   1120
3  1-1009, 1011-1019, 1021-1029, 1031-1039, 1041-1049, 1051-1059
   1061-1069, 1071-1079, 1081-1089, 1091-1099, 1101-1109, 1111-1119
   1121-4000
```

This example shows how to display the current configuration:

```
Router(config-mst)# show current
Current MST configuration
```
Name []
Revision 0
Instance VLANs mapped
-----------------------------------------------
0 1-4094
-----------------------------------------------

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Maps a VLAN or a set of VLANs to an MST instance.</td>
</tr>
<tr>
<td>name (MST configuration submode)</td>
<td>Sets the name of an MST region.</td>
</tr>
<tr>
<td>revision</td>
<td>Sets the revision number for the MST configuration.</td>
</tr>
<tr>
<td>show spanning-tree mst</td>
<td>Displays the information about the MST protocol.</td>
</tr>
<tr>
<td>spanning-tree mst configuration</td>
<td>Enters MST-configuration submode.</td>
</tr>
</tbody>
</table>

### show command append

To redirect and add the output of any `show` command to an existing file, use the `show command | append` command in privileged EXEC mode.

```
{show command | append url}
```

### Syntax Description

<table>
<thead>
<tr>
<th><code>command</code></th>
<th>Any Cisco IOS <code>show</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>`</td>
<td>append url`</td>
</tr>
<tr>
<td></td>
<td>The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include:</td>
</tr>
<tr>
<td></td>
<td>prefix:[directory]/filename</td>
</tr>
<tr>
<td></td>
<td>Prefixes can be local file locations, such as <code>flash</code> or <code>disk0</code>. Alternatively, you can specify network locations using the following syntax:</td>
</tr>
<tr>
<td></td>
<td><code>ftp: [[//]username [:@password]@]location ]/directory ]/filename</code></td>
</tr>
<tr>
<td></td>
<td><code>tftp: [[//]location ]/directory ]/filename</code></td>
</tr>
<tr>
<td></td>
<td>The rcp: prefix is not supported.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To display all URL prefixes that are supported for this command, use the `show command | append` command. This command adds the `show` command output to the end of the specified file.

Examples

In the following example, output from the `show tech-support` command is redirected to an existing file on Disk 1 with the file-name of “showoutput.txt.” This output is added at the end of any existing data in the file.

```
Router# show tech-support | append disk1:showoutput.txt
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show &lt;command&gt; redirect</code></td>
<td>Redirects the output of any <code>show</code> command to a specified file.</td>
</tr>
<tr>
<td></td>
<td><code>show &lt;command&gt; tee</code></td>
<td>Copies the <code>show</code> command output to a file while displaying it on the terminal.</td>
</tr>
</tbody>
</table>

**show command begin**

To begin the output of any `show` command from a specified string, use the `show command | begin` command in EXEC mode.

```
{show command | begin regular-expression}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>command</th>
<th>Any supported <code>show</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td></td>
<td><code>regular-expression</code></td>
<td>Any regular expression found in <code>show</code> command output. The show output will begin from the first instance of this string (output prior to this string will not be printed to the screen). The string is case-sensitive. Use parenthesis to indicate a literal use of spaces.</td>
</tr>
<tr>
<td></td>
<td><code>/</code></td>
<td>Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.</td>
</tr>
<tr>
<td></td>
<td><code>-</code></td>
<td>Specifies a filter at a --More-- prompt that only displays output lines that do not contain the regular expression.</td>
</tr>
<tr>
<td></td>
<td><code>+</code></td>
<td>Specifies a filter at a --More-- prompt that only displays output lines that contain the regular expression.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3</td>
<td>The <code>show</code> command was introduced.</td>
</tr>
<tr>
<td>12.0(1)T</td>
<td>This extension of the <code>show</code> command was introduced.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

The `regular-expression` argument is case sensitive and allows for complex matching requirements. Use parentheses to indicate a literal use of spaces. For example, `| begin u` indicates that the show output should begin with any line containing a `u`; `| begin ( u)` indicates that the show output should begin with any line that contains a space and a `u` together (line has a word that begins with a lowercase `u`).

To search the remaining output of the `show` command, use the following command at the `--More--` prompt:

```
/ regular-expression
```

You can specify a filtered search at any `--More--` prompt. To filter the remaining output of the `show` command, use one of the following commands at the `--More--` prompt:

- `regular-expression`
- `+ regular-expression`

When output volume is large, the search can produce long lists of output. To interrupt the output, press `Ctrl-^` (Ctrl-Shift-6) or `Ctrl-z`.

---

**Note**

Once you specify a filter for a `show` command, you cannot specify another filter at the next `--More--` prompt. The first specified filter remains until the `more` command output finishes or until you interrupt the output. The use of the keyword `begin` does not constitute a filter.

Because prior output is not saved, you cannot search or filter backward through prior output.

---

**Note**

A few `show` commands that have long output requirements do not require user input at the `--More--` prompt to jump to the next table of output; these types of output require you to enter the same number of `Ctrl-^` or `Ctrl-Z` combinations as there are `--More--` prompts to completely abort output.

---

### Examples

The following is partial sample output of the `show interface | begin Ethernet` command that begins unfiltered output with the first line that contains the regular expression “Ethernet.” At the `--More--` prompt, the user specifies a filter to show only the lines in the remaining output that contain the regular expression “Serial.”

```
Router# show interface | begin Ethernet
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
   Description: ip address is 172.1.2.14 255.255.255.0
   Internet address is 172.1.2.14/24
   .
   .
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
   --More--
   +Serial
   filtering...
```
Serial1 is up, line protocol is up
Serial2 is up, line protocol is up
Serial3 is up, line protocol is down
Serial4 is down, line protocol is down
Serial5 is up, line protocol is up
Serial6 is up, line protocol is up
Serial7 is up, line protocol is up

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>more &lt;url&gt; begin</td>
<td>Begins unfiltered output of the more command with the first line that contains the regular expression you specify.</td>
</tr>
<tr>
<td>more &lt;url&gt; exclude</td>
<td>Filters more command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>more &lt;url&gt; include</td>
<td>Filters more command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>show &lt;command&gt; exclude</td>
<td>Filters show command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>show &lt;command&gt; include</td>
<td>Filters show command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
</tbody>
</table>

### show command exclude

To filter show command output so that it excludes lines that contain a particular regular expression, use the `show command | exclude regular-expression` command in EXEC mode.

```bash
{show command|exclude regular-expression}
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>Any supported show command.</td>
</tr>
<tr>
<td></td>
<td>A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.</td>
</tr>
<tr>
<td>regular-expression</td>
<td>Any regular expression found in show command output.</td>
</tr>
<tr>
<td>/</td>
<td>Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.</td>
</tr>
</tbody>
</table>

#### Command Modes

EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The regular-expression argument is case sensitive and allows for complex matching requirements.
You can specify a new search at every --More-- prompt. To search the remaining output of the show command, use the following syntax at the --More-- prompt:

```
/ regular-expression
```

When output volume is large, the search can produce long lists of output. To interrupt the output, press Ctrl-^ (Ctrl-Shift-6) or Ctrl-Z.

Because prior output is not saved, you cannot search or filter backward through prior output.

---

**Note**
A few show commands that have long output requirements do not require user input at the --More-- prompt to jump to the next table of output; these types of output require you to enter the same number of Ctrl-^ or Ctrl-Z combinations as there are --More-- prompts to completely abort output.

---

### Examples

The following is partial sample output of the `show | exclude` command used with the `show buffers` command. It excludes lines that contain the regular expression “0 misses.” At the --More-- prompt, the user searches for the regular expression “Serial0,” which continues the filtered output with the first line that contains “Serial0.”

```
Router# show buffers | exclude 0 misses
Buffer elements:
  398 in free list (500 max allowed)
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
  50 in free list (20 min, 150 max allowed)
  551 hits, 3 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
  49 in free list (5 min, 150 max allowed)
Very Big buffers, 4520 bytes (total 10, permanent 10):
  
  
Huge buffers, 18024 bytes (total 0 permanent 0):
  0 in free list (0 min, 4 max allowed)
--More--
/Serial0
filtering...
Serial0 buffers, 1543 bytes (total 64, permanent 64):
  16 in free list (0 min, 64 max allowed)
  48 hits, 0 fallbacks
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>more &lt;url&gt; begin</td>
<td>Begins unfiltered output of the more command with the first line that contains the regular expression you specify.</td>
</tr>
<tr>
<td>more &lt;url&gt; exclude</td>
<td>Filters more command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>more &lt;url&gt; include</td>
<td>Filters more command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>show &lt;command&gt; begin</td>
<td>Searches the output of any show command and displays the output from the first instance of a specified string.</td>
</tr>
</tbody>
</table>
**show command include**

To filter `show` command output so that it only displays lines that contain a particular regular expression, use the `show command | include` command in EXEC mode.

```
{show command|include regular-expression}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>command</strong></td>
<td>Any supported <code>show</code> command.</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td><strong>regular-expression</strong></td>
<td>Any regular expression found in <code>show</code> command output. Use parenthesis to include spaces in the expression.</td>
</tr>
<tr>
<td><code>/</code></td>
<td>Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.</td>
</tr>
</tbody>
</table>

### Command Modes

**EXEC**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `regular-expression` argument is case sensitive and allows for complex matching requirements.

You can specify a new search at every --More-- prompt. To search the remaining output of the `show` command, use the following syntax at the --More-- prompt:

```
/ regular-expression
```

When output volume is large, the search can produce long lists of output. To interrupt the output, press `Ctrl-^` (Ctrl-Shift-6) or `Ctrl-Z`.

Because prior output is not saved, you cannot search or filter backward through prior output.

### Note

A few `show` commands that have long output requirements do not require user input at the --More-- prompt to jump to the next table of output; these types of output require you to enter the same number of Ctrl-^ or Ctrl-Z combinations as there are --More-- prompts to completely abort output.
Examples

The following is partial sample output of the `show interface | include ( is )` command. It displays only lines that contain the regular expression “( is ).” The parentheses force the inclusion of the spaces before and after “is.” Use of the parenthesis ensures that only lines containing “is” with a space both before and after it will be included in the output. Lines with words like “disconnect” will be excluded because there are not spaces around the instance of the string “is”.

```
Router# show interface | include ( is )
ATM0 is administratively down, line protocol is down
  Hardware is ATMizer BX-50
Dialer1 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
    DTR is pulsed for 1 seconds on reset
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
    Internet address is 172.21.53.199/24
Ethernet1 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.639c (bia 0060.837c.639c)
    Internet address is 5.5.5.99/24
Serial0:0 is down, line protocol is down
  Hardware is DSX1
.  
.  
--More--
```

At the `--More--` prompt, the user searches for the regular expression “Serial0:13”, which continues filtered output with the first line that contains “Serial0:13”.

```
/Serial0:13
filtering...
Serial0:13 is down, line protocol is down
  Hardware is DSX1
    Internet address is 11.0.0.2/8
      0 output errors, 0 collisions, 2 interface resets
    Timeslot(s) Used:14, Transmitter delay is 0 flags
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>more &lt;url&gt; begin</code></td>
<td>Begins unfiltered output of the <code>more</code> command with the first line that contains the regular expression you specify.</td>
</tr>
<tr>
<td><code>more &lt;url&gt; exclude</code></td>
<td>Filters <code>more</code> command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td><code>more &lt;url&gt; include</code></td>
<td>Filters <code>more</code> command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; begin</code></td>
<td>Searches the output of any <code>show</code> command and displays the output from the first instance of a specified string.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; exclude</code></td>
<td>Filters <code>show</code> command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
</tbody>
</table>
show command redirect

To redirect the output of any `show` command to a file, use the `show command | redirect` command in privileged EXEC mode.

```
{ show command|redirect url }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>command</strong></td>
<td>Any Cisco IOS <code>show</code> command.</td>
</tr>
<tr>
<td>**</td>
<td>redirect** <strong>url</strong></td>
</tr>
<tr>
<td></td>
<td>The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include:</td>
</tr>
<tr>
<td></td>
<td>prefix:[directory]/filename</td>
</tr>
<tr>
<td></td>
<td>Prefixes can be local file locations, such as <strong>flash</strong>: or <strong>disk0</strong>: Alternatively, you can specify network locations using the following syntax:</td>
</tr>
<tr>
<td></td>
<td>ftp: [/[/username [:password ]@]location ]/directory ]/filename</td>
</tr>
<tr>
<td></td>
<td>tftp: [/[/location ]/directory ]/filename</td>
</tr>
<tr>
<td></td>
<td>The <strong>rcp</strong>: prefix is not supported.</td>
</tr>
</tbody>
</table>

### Command Modes
- Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To display all URL prefixes that are supported for this command, use the `show command|redirect ?` command. This command creates a new file at the specified location, or overwrites an existing file.

### Examples

In the following example, output from the `show tech-support` command is write to the file “showtech.txt” on the host at 172.16.101.101 in the directory “/tftpboot/docs/” using FTP:

```
Router# show tech | redirect ftp://USER:MYPASSWORD@172.16.101.101/tftpboot/docs/showtech.txt
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show &lt;command&gt; append</code></td>
<td>Redirects and appends <code>show</code> command output to the end of an existing file.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; tee</code></td>
<td>Copies the <code>show</code> command output to a file while displaying it on the terminal.</td>
</tr>
</tbody>
</table>
show command section

To filter the output of a show command to match a given expression as well as any lines associated with that expression, use the `show command section` command in privileged EXEC mode.

```
{show command|section [{include|exclude}] regular-expression}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>Any Cisco IOS show command.</td>
</tr>
<tr>
<td>include</td>
<td>(Optional) Includes only the lines that contain a particular regular expression. This is the default keyword when none is specified.</td>
</tr>
<tr>
<td>exclude</td>
<td>(Optional) Excludes any lines that contain a particular regular expression.</td>
</tr>
<tr>
<td>regular-expression</td>
<td>Any regular expression or plain text string found in show command output. The syntax of the regular expression conforms to that of Bell V8 regexp(3).</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In many cases, it is useful to filter the output of a show command to match a specific expression. Filtering provides some control over the type and amount of information displayed by the system. The `show section` command provides enhanced filtering capabilities by matching lines in the show command output containing specific expressions as well as matching any entries associated with those expressions. Filtering is especially useful, for example, when displaying large configuration files using the `show running-configuration` command or the `show interfaces` command.

If the `include` or `exclude` keyword is not specified, `include` is the default.

If there are no associated entries for an expression, then only the line matching the expression is displayed.

**Examples**

The following examples compare the filtering characteristics of the `show running-config | include` command with the `show running-config | section` command. The first example gathers just the lines from the configuration file with “interface” in them.

```
Router# show running-config | include interface
interface Ethernet0/0
interface Ethernet1/0
interface Serial2/0
interface Serial3/0
```

The next example uses the `showcommand section` command to gather the lines in the configuration file with “interface” in them as well as any lines associated with those entries. In this example, interface configuration information is captured.

```
Router# show running-config | section include interface
interface Ethernet0/0
  shutdown
  no cdp enable
```
interface Ethernet1/0
shutdown
no cdp enable
interface Serial2/0
shutdown
no cdp enable
interface Serial3/0
shutdown
no cdp enable

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show &lt;command&gt; append</code></td>
<td>Redirects the output of any <code>show</code> command and adds it to the end of an existing file.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; exclude</code></td>
<td>Filters <code>show</code> command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; include</code></td>
<td>Filters <code>show</code> command output so that it displays only lines that contain a particular regular expression.</td>
</tr>
<tr>
<td><code>show &lt;command&gt; redirect</code></td>
<td>Redirects the output of any <code>show</code> command to a specified file.</td>
</tr>
</tbody>
</table>

### show command tee

To copy the output of any `show` command to a file while displaying it on the terminal, use the `show command tee` command in privileged EXEC mode.

```
{show command tee [/append] url}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>command</code></td>
<td>Any Cisco IOS <code>show</code> command.</td>
</tr>
</tbody>
</table>
| `tee` `url` | The addition of this syntax copies the command output to the file location specified in the Universal Resource Locator (URL). The pipe (|) is required. The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include:  
prefix|directory|filename  
Prefixes can be local file locations, such as `flash:` or `disk0:`. Alternatively, you can specify network locations using the following syntax:  
`ftp: ` [[/username [:password @]location ]/directory ]/filename  
`tftp: ` [[/location ]/directory ]/filename  
The `rcp:` prefix is not supported. |
| `/append` | (Optional) Adds the `show` command output to the end of an existing file. |

### Command Modes

Privileged EXEC
show (Flash file system)

To display the layout and contents of a Flash memory file system, use the `show flashfilesystem` command in EXEC mode.

**Class A Flash File Systems**

```
show flash-filesystem:[{all|chips|filesys}]
```

**Class B Flash File Systems**

```
show flash-filesystem:[partition-number:] [{all|chips|detailed|err|summary}]
```

**Class C Flash File Systems**

```
show flash-filesystem:
```
Syntax Description

**flash-fileystem**: Flash memory file system, followed by a colon. The availability of Flash file system keywords will vary by platform. Valid flash file system keywords include:

- `bootflash`
- `flash`
- `slot0`
- `slot1`
- `slavebootflash`
- `slaveslot0`
- `slaveslot1`

**all**: (Optional) On Class B Flash file systems, `all` keyword displays complete information about Flash memory, including information about the individual ROM devices in Flash memory and the names and sizes of all system image files stored in Flash memory, including those that are invalid.

On Class A Flash file systems, the `all` keyword displays the following information:

- The information displayed when no keywords are used.
- The information displayed by the `filesys` keyword.
- The information displayed by the `chips` keyword.

**chips**: (Optional) Displays information per partition and per chip, including which bank the chip is in, plus its code, size, and name.

**filesys**: (Optional) Displays the Device Info Block, the Status Info, and the Usage Info.

**partition-number**: (Optional) Displays output for the specified partition number. If you do not specify a partition in the command, the router displays output for all partitions. You can use this keyword only when Flash memory has multiple partitions.

**detailed**: (Optional) Displays detailed file directory information per partition, including file length, address, name, Flash memory checksum, computer checksum, bytes used, bytes available, total bytes, and bytes of system Flash memory.

**err**: (Optional) Displays write or erase failures in the form of number of retries.

**summary**: (Optional) Displays summary information per partition, including the partition size, bank size, state, and method by which files can be copied into a particular partition. You can use this keyword only when Flash memory has multiple partitions.

### Command Modes

**EXEC**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3</td>
<td>A timestamp that shows the offset from Coordinated Universal Time (UTC) was added to the <code>show</code> command display.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If Flash memory is partitioned, the command displays the requested output for each partition, unless you use the `partition` keyword.

The command also specifies the location of the current image.

To display the contents of boot Flash memory on Class A or B file systems, use the `show bootflash:` command as follows:

**Class A Flash file systems**

```
show bootflash: [all | chips | filesys]
```

**Class B Flash file systems**

```
show bootflash: [partition-number] [all | chips | detailed | err]
```

To display the contents of internal Flash memory on Class A or B file systems, use the `show flash:` command as follows:

**Class A Flash file systems**

```
show flash: all | chips | filesys]
```

**Class B Flash file systems**

```
show flash: [partition-number][all | chips | detailed | err | summary]
```

The `show(Flash file system)` command replaces the `show flash devices` command.

### Examples

The output of the `show` command depends on the type of Flash file system you select. Types include `flash;`, `bootflash;`, `slot0;`, `slot1;`, `slavebootflash;`, `slaveslot0;`, and `slaveslot1;`.

Examples of output from the `show flash` command are provided in the following sections:

- Class A Flash File System
- Class B Flash File Systems

Although the examples use `flash;` as the Flash file system, you may also use the other Flash file systems listed.

### Class A Flash File System

The following three examples show sample output for Class A Flash file systems. The table below describes the significant fields shown in the display.

The following is sample output from the `show flash:` command.

```
Router# show flash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1 .. unknown 317FBA1B 4A0694 24 4720148 Dec 15 2003 17:49:36 -08:00
```
Table 43: Show (Class A Flash File System) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Index number for the file.</td>
</tr>
<tr>
<td>ED</td>
<td>Whether the file contains an error (E) or is deleted (D).</td>
</tr>
<tr>
<td>type</td>
<td>File type (1 = configuration file, 2 = image file). The software displays these values only when the file type is certain. When the file type is unknown, the system displays “unknown” in this field.</td>
</tr>
<tr>
<td>crc</td>
<td>Cyclic redundant check for the file.</td>
</tr>
<tr>
<td>seek</td>
<td>Offset into the file system of the next file.</td>
</tr>
<tr>
<td>nlen</td>
<td>Name length—Length of the filename.</td>
</tr>
<tr>
<td>length</td>
<td>Length of the file itself.</td>
</tr>
<tr>
<td>date/time</td>
<td>Date and time the file was created. In the example, -08:00 indicates that the given date and time is 8 hours behind Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>name</td>
<td>Name of the file.</td>
</tr>
</tbody>
</table>

The following is sample output from the show flash: chips command:

```
RouterA# show flash: chips
******** Intel Series 2+ Status/Register Dump ********
ATTRIBUTE MEMORY REGISTERS:
 Config Option Reg (4000): 2
 Config Status Reg (4002): 0
 Card Status Reg (4100): 1
 Write Protect Reg (4104): 4
 Voltage Cntrl Reg (410C): 0
 Rdy/Busy Mode Reg (4140): 2
 COMMON MEMORY REGISTERS: Bank 0
 Intelligent ID Code : 8999A0A0
 Compatible Status Reg: B0B0
 Global Status Reg: B0B0
 Block Status Regs:
 0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
 8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
 16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
 24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
 COMMON MEMORY REGISTERS: Bank 1
 Intelligent ID Code : 8999A0A0
 Compatible Status Reg: B0B0
 Global Status Reg: B0B0
 Block Status Regs:
```

hampton/nitro/c7200-j-mz
2 .. unknown 9237F3FF 92C574E0 11 4767328 Jan 02 2004 18:42:53 -08:00 c7200-js-mz
3 .D unknown 71AB01F1 10C94E0 10 7982828 Jan 02 2004 18:48:14 -08:00 rsp-jsv-mz
4 .D unknown 96DACD45 10C97E0 8 639 Jan 03 2004 12:09:17 -08:00 the_time
5 .. unknown 96DACD45 10C9AE0 3 639 Jan 03 2004 12:09:32 -08:00 the_time
6 .D unknown 96DACD45 10C9DE0 8 639 Jan 03 2004 12:37:01 -08:00 the_time
7 .. unknown 96DACD45 10C9E0E0 8 639 Jan 03 2004 12:37:13 -08:00 the_time
3104544 bytes available (17473760 bytes used)
The following is sample output from the **show flash: filesys** command:

```
RouterA# show flash: filesys
-------- FILE SYSTEM STATUS --------
Device Number = 0

DETEC INFRO BLOfä:
Magic Number = 6887635  File System Vers = 10000  (1.0)
Length = 1400000  Sector Size = 20000
Programming Algorithm = 4  Erased State = FFFFFFFF
File System Offset = 20000  Length = 13A0000
MONLIB Offset = 100  Length = C730
Bad Sector Map Offset = 1FFEC  Length = 14
Squeeze Log Offset = 13C0000  Length = 20000
Squeeze Buffer Offset = 13E0000  Length = 20000
Num Spare Sectors = 0
Spares:

STATUS INFO:
Writable
NO File Open for Write
Complete Stats
No Unrecovered Errors
No Squeeze in progress

USAGE INFO:
Bytes Used = 10AA0E0  Bytes Available = 2F5F20
Bad Sectors = 0  Spared Sectors = 0
OK Files = 4  Bytes = 90C974
Deleted Files = 3  Bytes = 79D3EC
Files w/Errors = 0  Bytes = 0
```

The following is sample output from the **show flash:**command:
RouterB> show flash:

System flash directory:
File Length Name/status
1 4137888 c3640-c2is-mz.Feb24
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

The following example shows detailed information about the second partition in internal Flash memory:

RouterB# show flash:2

System flash directory, partition 2:
File Length Name/status
1 1711088 dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

Class B Flash File Systems

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addr</td>
<td>Address of the file in Flash memory.</td>
</tr>
<tr>
<td>available</td>
<td>Total number of bytes available in Flash memory.</td>
</tr>
<tr>
<td>Bank</td>
<td>Bank number.</td>
</tr>
<tr>
<td>Bank-Size</td>
<td>Size of bank in bytes.</td>
</tr>
<tr>
<td>bytes used</td>
<td>Total number of bytes used in Flash memory.</td>
</tr>
<tr>
<td>ccksum</td>
<td>Computed checksum.</td>
</tr>
<tr>
<td>Chip</td>
<td>Chip number.</td>
</tr>
<tr>
<td>Code</td>
<td>Code number.</td>
</tr>
<tr>
<td>Copy-Mode</td>
<td>Method by which the partition can be copied to:</td>
</tr>
<tr>
<td></td>
<td>• RXBOOT-MANUAL indicates a user can copy manually by reloading to the boot ROM image.</td>
</tr>
<tr>
<td></td>
<td>• RXBOOT-FLH indicates user can copy via Flash load helper.</td>
</tr>
<tr>
<td></td>
<td>• Direct indicates user can copy directly into Flash memory.</td>
</tr>
<tr>
<td></td>
<td>• None indicates that it is not possible to copy into that partition.</td>
</tr>
<tr>
<td>fcksum</td>
<td>Checksum recorded in Flash memory.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
File | Number of the system image file. If no filename is specified in the `boot system flash` command, the router boots the system image file with the lowest file number.
Free | Number of bytes free in partition.
Length | Size of the system image file (in bytes).
Name | Name of chip manufacturer and chip type.
Name/status | Filename and status of a system image file. The status [invalidated] appears when a file has been rewritten (recopied) into Flash memory. The first (now invalidated) copy of the file is still present within Flash memory, but it is rendered unusable in favor of the newest version. The [invalidated] status can also indicate an incomplete file that results from the user abnormally terminating the copy process, a network timeout, or a Flash memory overflow.
Partition | Partition number in Flash memory.
Size | Size of partition (in bytes) or size of chip.
State | State of the partition. It can be one of the following values:
- Read-Only indicates the partition that is being executed from.
- Read/Write is a partition that can be copied to.
System flash directory | Flash directory and its contents.
total | Total size of Flash memory (in bytes).
Used | Number of bytes used in partition.

The following is sample output from the `show flash: all` command:

```
RouterB> show flash: all
Partition Size Used Free Bank-Size State Copy Mode
1 16384K 4040K 12343K 4096K Read/Write Direct

System flash directory:
File Length Name/status add r ccksum ccksum
 1 4137952 bytes used, 12639264 available, 16777216 total
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

Chip Bank Code Size Name
1 1 01D5 1024KB AMD 29F080
2 1 01D5 1024KB AMD 29F080
3 1 01D5 1024KB AMD 29F080
4 1 01D5 1024KB AMD 29F080
1 2 01D5 1024KB AMD 29F080
2 2 01D5 1024KB AMD 29F080
3 2 01D5 1024KB AMD 29F080
4 2 01D5 1024KB AMD 29F080
1 3 01D5 1024KB AMD 29F080
```

Cisco IOS Configuration Fundamentals Command Reference
The following is sample output from the `show flash: all` command on a router with Flash memory partitioned:

```
Router# show flash: all
System flash partition information:
Partition
Size  Used  Free  Bank-Size  State  Copy-Mode
1     4096K 3459K 637K 4096K  Read Only  RXBOOT-FLH
2     4096K 3224K 872K 4096K  Read/Write  Direct

System flash directory, partition 1:
File Length Name/status
desc fcksum ccksum
1 3459720 master/igs-bfpx.100-4.3
0x40 0x3DE1 0x3DE1
[3459784 bytes used, 734520 available, 4194304 total]
4096K bytes of processor board System flash (Read ONLY)
Chip Bank Code Size Name
1 1 89A2 1024KB INTEL 28F008SA
2 1 89A2 1024KB INTEL 28F008SA
3 1 89A2 1024KB INTEL 28F008SA
4 1 89A2 1024KB INTEL 28F008SA
Executing current image from System flash [partition 1]

System flash directory, partition 2:
File Length Name/status
desc fcksum ccksum
1 3224008 igs-kf.100
0x40 0xEE91 0xEE91
[3224072 bytes used, 970232 available, 4194304 total]
4096K bytes of processor board System flash (Read/Write)
Chip Bank Code Size Name
1 2 89A2 1024KB INTEL 28F008SA
2 2 89A2 1024KB INTEL 28F008SA
3 2 89A2 1024KB INTEL 28F008SA
4 2 89A2 1024KB INTEL 28F008SA

The following is sample output from the `show flash: chips` command:

```
RouterB> show flash: chips
16384K bytes of processor board System flash (Read/Write)
Chip Bank Code Size Name
1 1 01D5 1024KB AMD 29F080
2 1 01D5 1024KB AMD 29F080
3 1 01D5 1024KB AMD 29F080
4 1 01D5 1024KB AMD 29F080
1 2 01D5 1024KB AMD 29F080
2 2 01D5 1024KB AMD 29F080
3 2 01D5 1024KB AMD 29F080
4 2 01D5 1024KB AMD 29F080
```
The following is sample output from the `show flash: detailed` command:

```
RouterB> show flash: detailed

System flash directory:
File Length Name/status
    addr fcksum ccksum
1 4137888 c3640-c2is-mz.Feb24 0x40 0xED65 0xED65
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

The following is sample output from the `show flash: err` command:

```
RouterB> show flash: err

System flash directory:
File Length Name/status
1 4137888 c3640-c2is-mz.Feb24
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

See the table above for a description of the fields. The `show flash: err` command also displays two extra fields: erase and write. The erase field indications the number of erase errors. The write field indicates the number of write errors.

The following is sample output from the `show flash summary` command on a router with Flash memory partitioned. The partition in the Read Only state is the partition from which the Cisco IOS image is being executed.

```
Router# show flash summary

System flash partition information:
Partition Size Used Free Bank-Size State Copy-Mode
1 4096K 2048K 2048K 2048K Read Only RXBOOT-FLH
2 4096K 2048K 2048K 2048K Read/Write Direct
```
show aliases

To display all alias commands, or the alias commands in a specified mode, use the **show aliases** command in EXEC mode.

```
show aliases [mode]
```

### Syntax Description

| **mode** | (Optional) Name of a specific command or configuration mode. Specifies that only aliases configured for this mode should be displayed. |

### Command Modes

**EXEC**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When used without the *mode* argument, this command will display all aliases currently configured on the system. Use the *mode* argument to display only the aliases configured for the specified command mode.

To display a list of the command mode keywords available for your system, use the **show aliases ?** command.

The following is sample output from the **show aliases exec** commands. The aliases configured for commands in EXEC mode are displayed.

```
Router> show aliases exec
Exec mode aliases:
 h help
 l lo logout
 p ping
 r resume
 s show
 w where
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>Creates a command alias.</td>
</tr>
</tbody>
</table>

show alignment

To display alignment errors and spurious memory access errors, use the **show alignment** command in privileged EXEC mode.

```
show alignment
```
Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(22)S.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Alignment Errors

Alignment errors are caused by misaligned reads and writes. For example, a two-byte read where the memory address is not an even multiple of two bytes is an alignment error. Alignment errors are caused by a software defect.

Alignment errors are reported in the system log and recorded by the device. Output from the `show alignment` command provides a record of these errors along with potentially useful traceback information. The traceback information for alignment errors can generally be decoded to reveal the function causing the alignment problems.

Spurious Memory Access Errors

Spurious memory access errors occur when a software process attempts to access memory in a restricted location. A read operation to this region of memory is usually caused when a nonexistent value is returned to a function in the software, or in other words, when a null pointer is passed to a function.

Spurious memory access errors are counted and recorded, if possible, by the software. This information is displayed with the `show alignment` command.

Examples

The following is sample output from the `show alignment` command when alignment detection is disabled. To enable alignment detection, use the `enable` command to enter privileged EXEC mode.

```
Device# show alignment
Unaligned handler is disabled
```

The following is sample output from the `show alignment` command when there are no alignment or spurious memory errors:

```
Device# show alignment
No alignment data has been recorded.
No spurious memory references have been recorded.
Device#
```

The following is sample output from the `show alignment` command when there are only alignment errors. The traceback information is necessary to determine the cause and the fix of the alignment errors.

```
Device# show alignment
Total Corrections 134, Recorded 1, Reads 134, Writes 0
Initial     Initial
```
The table below describes the significant fields shown in the display.

**Table 45: show alignment Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Corrections</td>
<td>Total number of alignment corrections made.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Number of alignment entries.</td>
</tr>
<tr>
<td>Reads</td>
<td>Number of misaligned reads.</td>
</tr>
<tr>
<td>Writes</td>
<td>Number of misaligned writes.</td>
</tr>
<tr>
<td>Initial Address</td>
<td>Address of where the alignment error occurred.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of times the alignment occurred at this address.</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Address of where the alignment error occurred.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of alignment error: read or write.</td>
</tr>
<tr>
<td>Traceback</td>
<td>The traceback address information necessary to determine the cause of the misalignment.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show alignment` command when there are only spurious memory access errors:

```
Device# show alignment
No alignment data has been recorded.
Total Spurious Accesses 50, Recorded 3
Address Count Traceback
E 10 0x605351A0 0x603CA084 0x606C4060 0x606D6368 0x60743284 0x60743270
E 20 0x605351A0 0x603EE7C 0x606C4060 0x606D6368 0x60743284 0x60743270
E 20 0x605351A0 0x603C99BC 0x606D53EC 0x606C4060 0x606D6368 0x60743284
Device#
```

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

**Table 46: show alignment Field Descriptions for Spurious Memory Access Errors**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Spurious Accesses</td>
<td>Total number of spurious memory accesses made.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Number of recorded spurious memory access entries.</td>
</tr>
<tr>
<td>Address</td>
<td>Address at which the spurious memory access error occurred.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of times the spurious memory access occurred at each address. The sum equals the Total Spurious Accesses.</td>
</tr>
<tr>
<td>Traceback</td>
<td>The traceback address information necessary to determine the cause of the misalignment.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show alignment` command when there are alignment errors and spurious memory access errors:

```
Device# show alignment
Total Corrections 134, Recorded 1, Reads 134, Writes 0
Initial Initial
Address Count Access Type Traceback
1A014C5 134 32bit read 0x6012F538 0x601338F8 0x601344D8 0x6022D528
Total Spurious Accesses 50, Recorded 3
Address Count Traceback
E 10 0x605351A0 0x603CA084 0x606D6368 0x60743284 0x60743270
E 20 0x605351A0 0x603EE7C 0x606D6368 0x60743284 0x60743270
E 20 0x605351A0 0x60398C 0x606D6368 0x60743284 0x60743270
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To enter privileged EXEC mode, or any other security level set by a system administrator, use the <code>enable</code> command in user EXEC or privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**show archive**

To display information about the files saved in the Cisco configuration archive, use the `show archive` command in privileged EXEC mode.

```
show archive
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show archive` command:
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
Archive # Name
0
1  disk0:myconfig-1 <- Most Recent
2
3
4
5
6
7
8
9
10
11
12
13
14

The following is sample output from the show archive command after several archive files of the running configuration have been saved. In this example, the maximum number of archive files to be saved is set to three.

Device# show archive
There are currently 3 archive configurations saved.
The next archive file will be named disk0:myconfig-8
Archive # Name
0
1  :Deleted
2  :Deleted
3  :Deleted
4  :Deleted
5  disk0:myconfig-5
6  disk0:myconfig-6
7  disk0:myconfig-7 <- Most Recent
8
9
10
11
12
13
14

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

Table 47: show archive Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive #</td>
<td>Indicates the number of the running configuration file saved to the Cisco configuration archive. You can set the maximum number of archive files of the running configuration to be saved in the configuration archive. The most recent archive file is the last one shown in the display.</td>
</tr>
<tr>
<td>Name</td>
<td>Indicates the name of the running configuration file saved to the Cisco configuration archive.</td>
</tr>
</tbody>
</table>
show archive config differences

To perform a line-by-line comparison of any two configuration files (accessible through the Cisco IOS File System [IFS]) and generate a list of the differences between them, use the `show archive config differences` command in user EXEC or privileged EXEC mode.

```
show archive config differences [filename1(path)[filename2(path)] [ignorecase]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filename1(path)</code></td>
<td>(Optional) The filename (path) of the first configuration file. Can be files in the following locations: bootflash:, cns:, fdp:, ftp:, harddisk:, http:, https:, null:, nvram:, obfl:, pram:, rcp:, revrcsf:, scp:, stby-bootflash:, stby-harddisk:, stby-nvram:, stby-obfl:, stby-rcsf:, stby-usb0:, stby-usb1:, system:, tar:, tftp:, tmpsys:, usb0:</td>
</tr>
<tr>
<td><code>filename2(path)</code></td>
<td>(Optional) The filename of the second configuration file. Can be files in the following locations: bootflash:, cns:, fdp:, ftp:, harddisk:, http:, https:, null:, nvram:, obfl:, pram:, rcp:, revrcsf:, scp:, stby-bootflash:, stby-harddisk:, stby-nvram:, stby-obfl:, stby-rcsf:, stby-usb0:, stby-usb1:, system:, tar:, tftp:, tmpsys:, usb0:</td>
</tr>
<tr>
<td><code>ignorecase</code></td>
<td>(Optional) Indicates that the case of the filenames should be ignored.</td>
</tr>
</tbody>
</table>

### Command Default

If the `filename1(path)` and `filename2(path)` arguments are not specified, the first configuration file is assumed to be the running configuration file and the second to be the startup configuration file.

If only the `filename1(path)` argument is specified, the second configuration file is assumed to be the running configuration file.

### Command Modes

User EXEC Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Interpreting the output of the `show archive config differences` command is dependent on the order in which the two files are configured. Each entry in the generated output list is prefixed with a unique text symbol to indicate the type of difference found. The text symbols and their meanings are as follows:

- A minus symbol (-) indicates that the configuration line exists in `filename1(path)` but not in `filename2(path)`.
- A plus symbol (+) indicates that the configuration line exists in `filename2(path)` but not in `filename1(path)`.
- An exclamation point (!) with descriptive comments is used to identify order-sensitive configuration lines whose location is different in `filename1(path)` than in `filename2(path)`.

Examples

In this example, a diff operation is performed on the running and startup configuration files. The table below shows the configuration files used for this example.

<table>
<thead>
<tr>
<th>Running Configuration File</th>
<th>Startup Configuration File</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no ip subnet-zero</code></td>
<td><code>ip subnet-zero</code></td>
</tr>
<tr>
<td><code>ip cef</code></td>
<td><code>ip cef</code></td>
</tr>
<tr>
<td><code>interface Ethernet1/0</code></td>
<td><code>ip name-server 10.4.4.4</code></td>
</tr>
<tr>
<td><code>ip address 10.7.7.255.0.0.0</code></td>
<td><code>voice dnis-map 1</code></td>
</tr>
<tr>
<td><code>no ip route-cache</code></td>
<td><code>dnis 111</code></td>
</tr>
<tr>
<td><code>no ip mroute-cache</code></td>
<td><code>interface Ethernet1/0</code></td>
</tr>
<tr>
<td><code>duplex half</code></td>
<td><code>no ip address</code></td>
</tr>
<tr>
<td><code>no ip classless</code></td>
<td><code>no ip route-cache</code></td>
</tr>
<tr>
<td><code>snmp-server community public RO</code></td>
<td><code>no ip mroute-cache</code></td>
</tr>
<tr>
<td></td>
<td><code>shutdown</code></td>
</tr>
<tr>
<td></td>
<td><code>duplex half</code></td>
</tr>
<tr>
<td></td>
<td><code>ip default-gateway 10.5.5.5</code></td>
</tr>
<tr>
<td></td>
<td><code>ip classless</code></td>
</tr>
<tr>
<td></td>
<td><code>access-list 110 deny ip any host 10.1.1.1</code></td>
</tr>
<tr>
<td></td>
<td><code>access-list 110 deny ip any host 10.1.1.2</code></td>
</tr>
<tr>
<td></td>
<td><code>access-list 110 deny ip any host 10.1.1.3</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server community private RW</code></td>
</tr>
</tbody>
</table>

The following is sample output from the `show archive config differences` command. This sample output displays the results of the diff operation performed on the configuration files in the table above.

```
Device# show archive config differences running-config startup-config
+ip subnet-zero
```
+ip name-server 10.4.4.4
+voice dnis-map 1
   +dnis 111
interface Ethernet1/0
+no ip address
+shutdown
+ip default-gateway 10.5.5.5
+ip classless
+access-list 110 deny ip any host 10.1.1.1
+access-list 110 deny ip any host 10.1.1.2
+access-list 110 deny ip any host 10.1.1.3
+snmp-server community private RW
-no ip subnet-zero
interface Ethernet1/0
- ip address 10.7.7.7 255.0.0.0
-no ip classless
- snmp-server community public RO

show archive config incremental-diffs

To perform a line-by-line comparison of a specified configuration file to the running configuration file and generate a list of the configuration lines that do not appear in the running configuration file, use the show archive config incremental-diffs command in user EXEC or privileged EXEC mode.

```
show archive config incremental-diffs file
```

**Syntax Description**

- `file` The filename of the configuration file to be compared to the running configuration file.

**Command Modes**

- User EXEC (>
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Modification

This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.

Release | Modification
--- | ---
12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
Cisco IOS XE Release 3.9S | This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

When an incremental diff operation is performed, a list of the configuration lines that do not appear in the running configuration file (in other words, configuration lines that only appear in the specified file that is being compared to the running configuration file) is generated as output. An exclamation point (!) with descriptive comments is used to identify order-sensitive configuration lines whose location is different in the specified configuration file than in the running configuration file.

Examples

In this example, an incremental diff operation is performed on the startup and running configuration files. The table below shows the configuration files used for this example.

Table 49: Configuration Files Used for the Incremental Diff Operation Example

<table>
<thead>
<tr>
<th>Startup Configuration File</th>
<th>Running Configuration File</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ip subnet-zero</td>
<td>no ip subnet-zero</td>
</tr>
<tr>
<td>ip cef</td>
<td>ip cef</td>
</tr>
<tr>
<td>ip name-server 10.4.4.4</td>
<td>interface Ethernet1/0</td>
</tr>
<tr>
<td>voice dnis-map 1</td>
<td>ip address 10.7.7.7 255.0.0.0</td>
</tr>
<tr>
<td>dnis 111</td>
<td>no ip route-cache</td>
</tr>
<tr>
<td>interface Ethernet1/0</td>
<td>no ip mroute-cache</td>
</tr>
<tr>
<td>no ip address</td>
<td>duplex half</td>
</tr>
<tr>
<td>no ip route-cache</td>
<td>no ip classless</td>
</tr>
<tr>
<td>no ip mroute-cache</td>
<td>snmp-server community public RO</td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>duplex half</td>
<td></td>
</tr>
<tr>
<td>ip default-gateway 10.5.5.5</td>
<td></td>
</tr>
<tr>
<td>ip classless</td>
<td></td>
</tr>
<tr>
<td>access-list 110 deny ip any host 10.1.1.1</td>
<td></td>
</tr>
<tr>
<td>access-list 110 deny ip any host 10.1.1.2</td>
<td></td>
</tr>
<tr>
<td>access-list 110 deny ip any host 10.1.1.3</td>
<td></td>
</tr>
<tr>
<td>snmp-server community private RW</td>
<td></td>
</tr>
</tbody>
</table>

The following is sample output from the `show archive config incremental-diffs` command. This sample output displays the results of the incremental diff operation performed on the configuration files in the above table.

Device# show archive config incremental-diffs nvram:startup-config
ip subnet-zero
ip name-server 10.4.4.4
voice dnis-map 1
dnis 111
interface Ethernet1/0
no ip address
shutdown
ip default-gateway 10.5.5.5
ip classless
access-list 110 deny ip any host 10.1.1.1
access-list 110 deny ip any host 10.1.1.2
access-list 110 deny ip any host 10.1.1.3
snmp-server community private RW

Cisco IOS Configuration Fundamentals Command Reference
access-list 110 deny ip any host 10.1.1.3
snmp-server community private RW

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>more nvram:startup-config</td>
<td>Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.</td>
</tr>
<tr>
<td></td>
<td>more system:running-config</td>
<td>Displays the contents of the currently running configuration file.</td>
</tr>
<tr>
<td></td>
<td>show archive config differences</td>
<td>Performs a line-by-line comparison of any two configuration files (accessible through the IFS) and generates a list of the differences between them.</td>
</tr>
</tbody>
</table>

**show archive config rollback timer**

To display settings of the timed rollback, use the `show archive config rollback timer` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced in Cisco IOS Release 12.4(15)T.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show archive config rollback timer` command to view the timed rollback settings, such as the timer type (idle timer or absolute timer), timer value, and so on, after a timed rollback is configured on a router.

**Examples**

The following is sample output from the `show archive config rollback timer` command:

```
Router# show archive config rollback timer
Time configured (or reconfigured): 22:50:48 UTC Sat Feb 21 2009
Timer type: absolute timer
Timer value: 2 min
User: console
```

The table below describes the significant fields in the sample output.
### Table 50: show mpls forwarding-table Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time configured (or reconfigured)</td>
<td>The time with which the timer refreshes every time the ENTER key is presses.</td>
</tr>
<tr>
<td>Timer type</td>
<td>The type of the timer: Idle or Absolute.</td>
</tr>
<tr>
<td>Timer value</td>
<td>Displays the time, in minutes, for which to wait for confirmation.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the user name.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure revert</td>
<td>Cancels the timed rollback and trigger the rollback immediately or resets parameters for the timed rollback.</td>
</tr>
<tr>
<td>configure terminal revert timer</td>
<td>Enter global configuration mode and sets the parameters for reverting the configuration if confirmation of the new configuration is not received.</td>
</tr>
</tbody>
</table>

### show archive log config

To display entries from the configuration log, use the `show archive log config` command in privileged EXEC mode.

```
show archive log config {all}record-number [end-number]user username [session session-number]record-number [end-number]|statistics| [provisioning] [contenttype {plaintext|xml}] [persistent]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all configuration log entries.</td>
</tr>
<tr>
<td>record-number [end-number]</td>
<td>Displays the log entry by record number. If you specify a record number for the optional <code>end-number</code> argument, all log entries with record numbers between the values entered for the <code>record-number</code> and <code>end-number</code> arguments are displayed. Valid values for the <code>record-number</code> and <code>end-number</code> arguments range from 1 to 2147483647.</td>
</tr>
<tr>
<td>user username</td>
<td>Displays log entries attributed to a particular user.</td>
</tr>
<tr>
<td>session session-number</td>
<td>(Optional) Displays log entries attributed to a particular session. Valid values for the <code>session-number</code> argument range from 1 to 1000.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays memory usage information for the configuration log.</td>
</tr>
<tr>
<td>provisioning</td>
<td>(Optional) Displays configuration log file information as it would appear in a configuration file, rather than in tabular format.</td>
</tr>
<tr>
<td>contenttype</td>
<td>(Optional) Specifies the format for the display of configuration change results.</td>
</tr>
<tr>
<td>plaintext</td>
<td>Specifies that the configuration change results will be formatted as plain text. This keyword appears only if the <code>contenttype</code> keyword has been entered.</td>
</tr>
</tbody>
</table>
xml | Specifies that the configuration change results will be in eXtensible Markup Language (XML) format. This keyword appears only if the `contenttype` keyword has been entered.

persistent | (Optional) Displays the persistent configuration changes in a configlet format.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>The <code>contenttype</code>, <code>plaintext</code>, <code>xml</code>, and <code>persistent</code> keywords were added.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command with syntax updated in 12.2(33)SRA was integrated into Cisco</td>
</tr>
<tr>
<td></td>
<td>IOS Release 12.2(33)SB. This command was implemented on the Cisco 10000</td>
</tr>
<tr>
<td></td>
<td>series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you do not specify the `all` keyword, you must specify a record number with the `record-number` argument. You can optionally specify an end record number with the `end-number` argument to display a range of records. If you use the `end-number` argument to specify a record number that does not exist, all records after the starting record number with a record number lower than that specified with the `end-number` argument are displayed.

Specifying the `provisioning` keyword results in the display appearing as it would in a configuration file, rather than in tabular format. This output includes commands used to change configuration modes and logged configuration commands. This output can be used to set up another device if desired.

### Note

Any command that is configured internally and not through the standard method such as entered by the user on the console or by copy command will not be logged in the archive logger buffer. Such commands are not shown as a part of the `show archive log config all` command output.

### Examples

The following is sample output from the `show archive log config` command, which displays configuration log entry numbers 1 and 2:

```
Device# show archive log config 1 2
idx  sess  user@line  Logged command
 1   1    user1@console logging enable
 2   1    user1@console logging size 200
```

The table below describes the significant fields shown in the display.
Table 51: show archive log config Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idx</td>
<td>The record number of the configuration log entry.</td>
</tr>
<tr>
<td>sess</td>
<td>The session number associated with the configuration log entry.</td>
</tr>
<tr>
<td>user@line</td>
<td>The username of the user who executed the command that generated the configuration log entry.</td>
</tr>
<tr>
<td>Logged command</td>
<td>The command that was executed.</td>
</tr>
</tbody>
</table>

The following example results in the display of all configuration log files as they would appear in a configuration file rather than in tabular format. In addition to displaying logged commands, the example shows the commands used to change configuration modes that are required to correctly apply the logged commands.

Device# `show archive log config all provisioning
archive
log config
logging enable
logging size 200`

The following example results in the display of memory usage statistics for the configuration log:

Device# `show archive log config statistics`
Config Log Session Info:
Number of sessions being tracked: 1
Memory being held: 3910 bytes
Total memory allocated for session tracking: 3910 bytes
Total memory freed from session tracking: 0 bytes
Config Log log-queue Info:
Number of entries in the log-queue: 3
Memory being held in the log-queue: 671 bytes
Total memory allocated for log entries: 671 bytes
Total memory freed from log entries:: 0 bytes

The output is self-explanatory.

The following example shows the contents of the archive log in XML format:

Device# `show archive log config all contenttype xml`<configLoggerMsg version="1.0" encoding="UTF-8">   
<configChanged>  
<changeInfo>  
  <user>jdoe</user>  
  <async>  
    <port>con_0</port>  
  </async>  
<when>  
</when>  
</changeInfo>  
<logComment>begin test test1</logComment>  
</configChanged>  
<configChanged>  
<changeInfo>
**show as5400**

To display the hardware details of an application server, use the `show as5400` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show as5400` command provides complex troubleshooting information that pertains to the platform's shared references rather than to a specific interface.

**Examples**

The following is sample output from the `show as5400` command:

```
Router# show as5400
Hardware Info:
System I/O Controller PLD version: 0x8
Serial Interface Controller PLD version: 0x2
Memory Info:
Memory Installed: 1024 MB
Memory Type is : DDR
Bus Watcher Counters
cor_l2cache_data_ecc_count = 0
bad_l2cache_data_ecc_count = 0
cor_l2cache_tag_ecc_count = 0
bad_l2cache_tag_ecc_count = 0
cor_memory_data_ecc_count = 0
bad_memory_data_ecc_count = 0
bus_errors = 0
System Controller Network Interrupts:
Interrupt Register is at 0xB0020040 (0x0000008000000000)
BCM interrupt mask 0xFF7C03BEFF0FCC2
Registered Interrupts:
<table>
<thead>
<tr>
<th>Level Mask</th>
<th>Count</th>
<th>Data</th>
<th>Interrupt Handler</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0x0000000000000000 0</td>
<td>0x00000000 0x6036C144 (GT96124 Interrupt h)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0x0000000000000000 0</td>
<td>0x0C97F6AC 0x60354064 (GigabitEthernet0/1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0x0000000000000000 0</td>
<td>0x66712B8C 0x60354064 (GigabitEthernet0/0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0x0000000000000000 0</td>
<td>0x66712B8C 0x60354064 (Low IRQ interrupt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0x0000100000000000 0</td>
<td>0x00000000 0x6085D98 (BCM1125 GPIO12 - BI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0x0000000000000000 0</td>
<td>0x00000000 0x6085D98 (BCM1125 Timer 3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0x0000000000000000 0</td>
<td>0x00000000 0x6085D98 (BCM1125 Timer 2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0x0000000000000000 0</td>
<td>0x00000000 0x6085D98 (BCM1125 Timer 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0x0000000000000000 0</td>
<td>0x00000000 0x6085D98 (BCM1125 Timer 0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0x0000000000000000 0</td>
<td>0x00000000 0x6085D98 (HighIRQ interrupt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 0x0000000000000000 0</td>
<td>0x00000000 0x60380F88 (OIR Interrupt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 0x0000000000000000 0</td>
<td>0x00000000 0x608B2FCB (NRBUS Parity Error)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 0x0000000000000000 0</td>
<td>0x00000000 0x608B2FCB (IO Error)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Address</th>
<th>Value</th>
<th>Address</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000004000000000</td>
<td>0x00000000</td>
<td>0x00000000</td>
<td>0x608BD1EC</td>
</tr>
<tr>
<td>0x007C000000000000</td>
<td>0x00080F00</td>
<td>0x00000000</td>
<td>0x608C2FD8</td>
</tr>
<tr>
<td>0x0000000000020000</td>
<td>0x00000000</td>
<td>0x00080C3A14</td>
<td>0x608C3A14</td>
</tr>
<tr>
<td>0x0000000000010000</td>
<td>0x00000000</td>
<td>0x00080C2A7C</td>
<td>0x608C2A7C</td>
</tr>
<tr>
<td>0x0000000000400000</td>
<td>0x00000000</td>
<td>0x649858BC</td>
<td>0x608C2B4C</td>
</tr>
<tr>
<td>0x0000000000000000</td>
<td>0x00000000</td>
<td>0x00000000</td>
<td>0x608C2E04</td>
</tr>
<tr>
<td>0x0000000000000000</td>
<td>0x00000000</td>
<td>0x00000000</td>
<td>0x608C28D4</td>
</tr>
<tr>
<td>0x0000000000000000</td>
<td>0x00000000</td>
<td>0x00000000</td>
<td>0x608C2FD8</td>
</tr>
</tbody>
</table>

HT 600MHz Retry Count 0

BCM1125H HT Host Bridge, handle=0

BCM bridge, config=0x0
(0x00):dev, vendor id = 0x0002166D
(0x04):status, command = 0x00100107
(0x08):class code, revid = 0x06000003
(0x0C):hdr, lat timer, cls = 0x00010000
(0x18):bus id registers = 0x001B0100
(0x1C):secondary status = 0x00000141
(0x20):mem base/limit = 0x5FF04300
(0x30):io upper limit/base = 0x00010000
(0x34):capabilities ptr = 0x00000040
(0x38):expansion rom bar = 0x00000000
(0x3C):bridge ctrl = 0x00020000
(0x40):LDT cmd, cap id, = 0x20000008
(0x44):Link config/control = 0x00000020
(0x48):Link frequency = 0x801F0423
(0x50):SRICmd, srirxden, srirxden = 0x50211010
(0x54):SRI tx numerator = 0x0000FFFF
(0x58):SRI rx numerator = 0x0000FFFF
(0x60):Error status/control = 0x00090A99
(0x64):Tx ctrl, databufalloc = 0x00041515
(0x68):Rx CRC expected = 0xBFFFABE0
(0x70):Rx CRC received = 0x7FF3FFFD

BCM PCI Host Bridge:

DeviceID=0x0001, VendorID=0x166D, Cmd=0x0146, Status=0x02A0
Cls=0x06/0x00/0x00, Rev=0x03, LatencyTimer=0x2C, CacheLineSize=0x10
BaseAddr0=0x60000008, BaseAddr1=0x00000000, MaxLat=0x00, MinGnt=0x00
SubsysDeviceID=0x0000, SubsysVendorID=0xFFFF, ErrorAddr=0x00030400
Additional Status = 0x00000020

PLX HT2PCI Bridge A for PCM Tracer & DFC 2,4,6, handle=0

PLX HT7520 bridge, config=0x0
(0x00):dev, vendor id = 0x74501022
(0x04):status, command = 0x02300107
(0x08):class code, revid = 0x06040012
(0x0C):hdr, lat timer, cls = 0x00810000
(0x18):bus id registers = 0xF80E0201
(0x1C):secondary status = 0x02200141
(0x20):mem base/limit = 0x4FF04300
(0x30):io upper limit/base = 0x00010000
(0x34):capabilities ptr = 0x000000A0
(0x38):bridge ctrl = 0x00020000
(0x3C):miscellaneous = 0x00010004
(0x40):prefetch ctrl = 0x00000046
(0x44):ht cmd, cap id = 0x00041008
(0x48):link cfg/ctrl side a = 0x00112020
(0x4C):link cfg/ctrl side b = 0x770020D0
(0x50):link freq ctrl side a = 0x00350422
(0x54):link freq ctrl side b = 0x00350402

PLX HT2PCI Bridge B, for DFC 1,3,5,7
(0x00):dev, vendor id = 0x74501022
(0x04):status, command = 0x02300107
(0x08):class code, revid = 0x06040012
(0x0C):hdr, lat timer, cls = 0x00810000

Cisco IOS Configuration Fundamentals Command Reference
The table below describes the significant fields shown in the display.

### Table 52: show as5400 Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System I/O Controller PLD version</td>
<td>The version of the programmable logic device (PLD) on the system.</td>
</tr>
<tr>
<td>Level</td>
<td>Interrupt priority level.</td>
</tr>
<tr>
<td>Mask</td>
<td>Maskable interrupt.</td>
</tr>
<tr>
<td>Count</td>
<td>Interrupt count.</td>
</tr>
<tr>
<td>Handler</td>
<td>Type of interrupt handler.</td>
</tr>
<tr>
<td>RTC chip</td>
<td>Real time clock chip type.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as</td>
<td>Defines an application server on a gateway.</td>
</tr>
</tbody>
</table>

### show async bootp

To display the extended BOOTP request parameters that have been configured for asynchronous interfaces, use the `show async bootp` command in privileged EXEC mode.

**show async bootp**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show async bootp` command:

```
Router# show async bootp
```
show async bootp

The following extended data will be sent in BOOTP responses:
bootfile (for address 192.168.1.1) “pcboot”
bootfile (for address 172.16.1.111) “dirtboot”
subnet-mask 255.255.0.0
time-offset -3600
time-server 192.168.1.1

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootfile... “pcboot”</td>
<td>Boot file for address 192.168.1.1 is named pcboot.</td>
</tr>
<tr>
<td>subnet-mask 255.255.0.0</td>
<td>Subnet mask.</td>
</tr>
<tr>
<td>time-offset -3600</td>
<td>Local time is one hour (3600 seconds) earlier than UTC time.</td>
</tr>
<tr>
<td>time-server 192.168.1.1</td>
<td>Address of the time server for the network.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>async-bootp</td>
<td>Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.</td>
</tr>
</tbody>
</table>

**show autoupgrade configuration unknown**

To display all of the unknown start-up configuration lines that the auto-upgraded Cisco software image does not understand, use the **show autoupgrade configuration unknown** command in privileged EXEC mode.

**show autoupgrade configuration unknown**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **show autoupgrade configuration unknown** command to view any invalid start-up configuration. This command prints invalid start-up configuration data only when run from an image which was upgraded using the Cisco IOS Auto-Upgrade Manager (AUM). This command output is useful when you are upgrading to an image with a different feature set.

**Examples**

The following example shows how to view the invalid start-up configuration lines that the Cisco software image, upgraded on the device using AUM, does not understand:
Device# show autoupgrade configuration unknown
! Config Lines not understood by the current image:
voice-card 0
no dspfarm
crypto pki trustpoint aum_cisco_ca
enrollment terminal
revocation-check none
crypto pki certificate chain aum_cisco_ca
certificate ca 40DCB71E54EE24CBE5326F8006BBA4F6 nvram:SecureServer#A4F6CA.cer
no ip http secure-server
transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh

Total 9 Invalid Config Lines

Device#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrade automatic abortversion</td>
<td>Cancels a scheduled reloading of the device with a new Cisco software image.</td>
</tr>
<tr>
<td>upgrade automatic getversion</td>
<td>Downloads a Cisco software image directly from <a href="http://www.cisco.com">www.cisco.com</a> or from a non-Cisco server.</td>
</tr>
<tr>
<td>upgrade automatic runversion</td>
<td>Reloads the device with a new Cisco software image.</td>
</tr>
</tbody>
</table>

### show bcm560x

To display the BCM560x hardware table information, use the `show bcm560x` command in user EXEC or privileged EXEC mode.

`show bcm560x name {offset|all} [raw]`

**Syntax Description**

- **name**: Displays the bcm50x hardware table name. The hardware table name can be VLAN table name (VTABLE) or Port based VLAN table name (PTABLE):
- **offset**: Hardware table number. Range is from 0 to 65535
- **all**: Displays all the bcm560x hardware table names.
- **raw**: (Optional) Displays the bcm560x hardware table names.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.4(15)T.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bcm560x all` command:

```
Router# show bcm560x VTABLE all
```
show bootflash:

To display information about the bootflash: file system, use the `show bootflash:` command in user EXEC or privileged EXEC mode.

```
show bootflash: [{all|chips|filesys}]
```

**Syntax Description**

- **all** (Optional) Displays all possible Flash information.
- **chips** (Optional) Displays information about the Flash chip.
- **filesys** (Optional) Displays information about the file system.

**Command Default**

This command has no default settings.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display information about the file system status:

```
Router> show bootflash: filesys
-------- F I L E S Y S T E M S T A T U S --------
    Device Number = 0
    DEVICE INFO BLOCK: bootflash
        Magic Number = 6887635    File System Vers = 10000 (1.0)
        Length = 10000000    Sector Size = 40000
        Programming Algorithm = 39    Erased State = FFFFFFFF
        File System Offset = 40000    Length = F40000
        MCNLIB Offset = 100    Length = C628
        Bad Sector Map Offset = 3FFFFFF
        Squeeze Log Offset = F800000    Length = 40000
        Squeeze Buffer Offset = FC000000    Length = 40000
        Num Spare Sectors = 0
    Spares:
    STATUS INFO:
        Writable
        NO File Open for Write
```
Complete Stats
No Unrecovered Errors
No Squeeze in progress

USAGE INFO:
Bytes Used = 917CE8  Bytes Available = 628318
Bad Sectors = 0     Spared Sectors = 0
OK Files    = 2     Bytes = 917BE8
Deleted Files = 0   Bytes = 0
Files w/Errors = 0  Bytes = 0

Router>

This example shows how to display image information:

Router>
show bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1 .. image 8C5A393A 237E3C 14 2063804 Aug 23 1999 16:18:45 c6msfc-boot-mz
2 .. image D86EE0AD 957CE8 9 7470636 Sep 20 1999 13:48:49 rp.halley

Router>

This example shows how to display all bootflash information:

Router>
show bootflash: all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1 .. image 8C5A393A 237E3C 14 2063804 Aug 23 1999 16:18:45 c6msfc-boot-mz
2 .. image D86EE0AD 957CE8 9 7470636 Sep 20 1999 13:48:49 rp.halley
6456088 bytes available (9534696 bytes used)

-------- F I L E S Y S T E M S T A T U S --------
Device Number = 0

DEVICE INFO BLOCK: bootflash
Magic Number = 6887635  File System Vers = 10000  (1.0)
Length = 1000000  Sector Size = 40000
Programming Algorithm = 39  Erased State = FFFFFFFF
File System Offset = 40000  Length = F40000
MONLIB Offset = 100  Length = C628
Bad Sector Map Offset = 3FF8  Length = 8
Squeeze Log Offset = F80000  Length = 40000
Squeeze Buffer Offset = FC0000  Length = 40000
Num Spare Sectors = 0

Spare:

STATUS INFO:
Writable
NO File Open for Write
Complete Stats
No Unrecovered Errors
No Squeeze in progress

USAGE INFO:
Bytes Used = 917CE8  Bytes Available = 628318
Bad Sectors = 0     Spared Sectors = 0
OK Files    = 2     Bytes = 917BE8
Deleted Files = 0   Bytes = 0
Files w/Errors = 0  Bytes = 0

Router>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Marks files on bootflash for deletion.</td>
</tr>
<tr>
<td>squeeze</td>
<td>Removes files from bootflash that have been marked for deletion.</td>
</tr>
</tbody>
</table>
show bootvar

To display the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting, use the show bootvar command in user EXEC or privileged EXEC mode.

show bootvar

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was integrated into Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Supported Platforms Other than the Cisco 7600 Series Router

The show bootvar command replaces the show boot command.

The show bootvar command allows you to view the current settings for the following variables:

- BOOT
- CONFIG_FILE
- BOOTLDR

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. The BOOTLDR variable specifies the flash device and filename containing the rxboot image that ROM uses for booting. You set these variables with the boot system, boot config, and boot bootldr global configuration commands, respectively.

When you use this command on a device with multiple Route Switch Processor (RSP) cards (Dual RSPs), this command also shows you the variable settings for both the master and slave RSP card.

Cisco 7600 Series Router

The show bootvar command displays information about the BOOT environmental variable.

The command output depends on how you configure the boot statement as follows:

- If you enter the boot system flash bootflash: sup720_image command in the boot configuration, then the show bootvar command output displays the bootflash information.

- If you enter the boot system flash sup-bootflash: sup720_image command in the boot configuration, then the show bootvar command output displays the sup-bootflash information. This action is the correct way of configuring the boot statement.
The `show bootvar` command is available from the switch processor command-line interface (CLI) and the route processor CLI. From the switch processor CLI, the display is always bootflash. With either the bootflash or the sup-bootflash boot statement, the switch boots correctly. You should use sup-bootflash in the boot configuration statement because the image is stored in the switch processor bootflash; the route processor sees the image as sup-bootflash.

The number displayed after the image name (for example, c6sup12-js-mz.121-13.E1,12) indicates the number of times that the Cisco 7600 series router tries to reboot the file before giving up.

### Examples

#### Supported Platforms Other than the Cisco 7600 Series Router

The following is sample output from the `show bootvar` command:

```
Router# show bootvar
BOOT variable =
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = slot0:router-config
BOOTLDR variable not exist
Configuration register is 0x0
```

In this example, the BOOT variable contains a null string; that is no bootable images are specified.

The CONFIG_FILE variable points to the configuration file in NVRAM as the startup (initialization) configuration. The run-time value for the CONFIG_FILE variable points to the router-configuration file on the flash memory card inserted in the first slot of the RSP card. That is, during the run-time configuration, you have modified the CONFIG_FILE variable using the `boot config` command, but you have not saved the run-time configuration to the startup configuration. To save your run-time configuration to the startup configuration, use the `copy system:running-config nvram:startup-config` command. If you do not save the run-time configuration to the startup configuration, then the system reverts to the saved CONFIG_FILE variable setting for initialization information upon reload. In this sample, the system reverts to NVRAM for the startup configuration file.

The BOOTLDR variable does not yet exist. That is, you have not created the BOOTLDR variable using the `boot bootldr` global configuration command.

The following example is output from the `show bootvar` command for a Cisco 7513 router configured for high system availability (HSA):

```
Router# show bootvar
BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x0
current slave is in slot 7
BOOT variable =
CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x0
```

The table below describes the significant fields shown in the displays.
Table 54: show bootvar Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT variable</td>
<td>Displays a list of specified bootable images.</td>
</tr>
<tr>
<td>CONFIG_FILE variable</td>
<td>Indicates where to locate the startup (initialization) configuration file.</td>
</tr>
<tr>
<td>Current CONFIG_FILE variable</td>
<td>Identifies the run-time configuration file.</td>
</tr>
<tr>
<td>BOOTLDR variable</td>
<td>Identifies the location of the boot image that ROM uses for booting, if it is specified.</td>
</tr>
<tr>
<td>Configuration register</td>
<td>Specifies router behavior, such as how the router boots, options while booting, and console speed (baud rate for a terminal emulation session).</td>
</tr>
<tr>
<td>current slave is in slot 7</td>
<td>Indicates the slot where the redundant system is located in HSA configurations.</td>
</tr>
</tbody>
</table>

Cisco 7600 Series Router

This example shows how to display information about the BOOT environment variable:

```
Router# show bootvar
BOOT variable = sup-bootflash:c6sup12-js-mz.121-13.E,12
CONFIG_FILE variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Configuration register is 0x2102
Standby has 112640K/18432K bytes of memory.
Standby BOOT variable = bootflash:c6sup12-js-mz.121-13.E,12
Standby CONFIG_FILE variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Standby BOOTLDR variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Standby Configuration register is 0x2102
```

The number displayed after the image name (for example, c6sup12-js-mz.121-13.E,12) indicates the number of times that the Cisco 7600 series router tries to reboot the file before giving up.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot bootldr</td>
<td>Specifies the location of the boot image that ROM uses for booting.</td>
</tr>
<tr>
<td>boot bootstrap</td>
<td>Configures the filename that is used to boot a secondary bootstrap image.</td>
</tr>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).</td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the system image that the router loads at startup.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies a file from source to a destination.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.</td>
</tr>
</tbody>
</table>
**show buffers**

To display detailed information about the buffer pools on the network server when Cisco IOS, Cisco IOS Software Modularity, or Cisco IOS XE images are running, use the `show buffers` command in user EXEC or privileged EXEC mode.

```
show buffers [{address  hex-address|failures|pool  pool-name|detailed|processes|all|assigned [process-id]|free|old|input-interface  interface-type  interface-number} {[pool  pool-name}] [{dump|header|packet|location  pool-location}]]
```

---

**Cisco Catalyst 4500e Series Switches running IOS XE software**

```
show buffers [detailed  process-id] {address  hex-address|all|assigned|failures|free|input-interface  interface-type  interface-number|old|pool  pool-name}  [{dump|header|packet|location  pool-location}]]
```

---

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address</strong></td>
<td>(Optional) Displays buffers at a specified address.</td>
</tr>
<tr>
<td><strong>hex-address</strong></td>
<td>(Optional) Address in hexadecimal notation.</td>
</tr>
<tr>
<td><strong>failures</strong></td>
<td>(Optional) Displays buffer allocation failures.</td>
</tr>
<tr>
<td><strong>pool</strong></td>
<td>(Optional) Displays buffers in a specified buffer pool.</td>
</tr>
<tr>
<td><strong>pool-name</strong></td>
<td>(Optional) Name of buffer pool.</td>
</tr>
<tr>
<td><strong>detailed process</strong></td>
<td>(Optional) Displays detailed buffer information.</td>
</tr>
<tr>
<td><strong>processes</strong></td>
<td>(Optional) For Cisco IOS Software Modularity images only. Displays buffers connected to Packet Manager.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>(Optional) Displays all buffers.</td>
</tr>
<tr>
<td><strong>assigned</strong></td>
<td>(Optional) Displays the buffers in use.</td>
</tr>
<tr>
<td><strong>process-id</strong></td>
<td>(Optional) For Cisco IOS Software Modularity images only. POSIX process identifier.</td>
</tr>
<tr>
<td><strong>free</strong></td>
<td>(Optional) Displays the buffers available for use.</td>
</tr>
<tr>
<td><strong>old</strong></td>
<td>(Optional) Displays buffers older than one minute.</td>
</tr>
<tr>
<td><strong>input-interface</strong></td>
<td>(Optional) Displays interface pool information. If an interface type is specified and this interface has its own buffer pool, information for that pool is displayed.</td>
</tr>
<tr>
<td><strong>interface-type</strong></td>
<td>(Optional) Interface type.</td>
</tr>
<tr>
<td><strong>interface-number</strong></td>
<td>(Optional) Interface number.</td>
</tr>
<tr>
<td><strong>dump</strong></td>
<td>(Optional) Displays the buffer header and all data.</td>
</tr>
<tr>
<td><strong>header</strong></td>
<td>(Optional) Displays the buffer header only.</td>
</tr>
<tr>
<td><strong>packet</strong></td>
<td>(Optional) Displays the buffer header and packet data.</td>
</tr>
</tbody>
</table>
location pool-location  (Optional) Displays all the buffer pools in a given location. The global buffer pools come first, followed up with process-level buffer pools.

Usage Guidelines

When you use the show buffers input-interface [packet | dump] command, some of the data packets are not displayed correctly because of the way packets are assembled for display on the CLI.

Pointers to the memory location of the header and data for the packet are stored in local memory. By the time the pointers are de-referenced, it is possible that the memory storing the header or packet data is overwritten. For example, in the show buffers input-interface packet command output, the source and destination addresses might not match the actual source and destination address if the packet data were decoded by some secondary means such as analyzing manually or by other means. It is recommended that the users of this command must validate packets by a secondary means.

Command Default

If no options are specified, all buffer pool information is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3</td>
<td>The option to filter display output based on specific buffer pools was expanded.</td>
</tr>
<tr>
<td>12.2(18)SXF4</td>
<td>Two additional fields were added to the output to support Cisco IOS Software Modularity.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1.0.SG</td>
<td>This command was introduced on the Cisco Catalyst 4500e Series Switches with support for the detailed process command option.</td>
</tr>
</tbody>
</table>

Cisco IOS Software

The following is sample output from the show buffers command with no arguments, showing all buffer pool information:

Router# show buffers
Buffer elements:
    398 in free list (500 max allowed)
    1266 hits, 0 misses, 0 created
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
    50 in free list (20 min, 150 max allowed)
    551 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 25, permanent 25):
    25 in free list (10 min, 150 max allowed)
The following is sample output from the `show buffers` command with no arguments, showing only buffer pool information for Huge buffers. This output shows a highest total of five Huge buffers created five days and 18 hours before the command was issued.

Router# show buffers
Huge buffers, 18024 bytes (total 5, permanent 0, peak 5 @ 5d18h):
  4 in free list (3 min, 104 max allowed)
  0 hits, 1 misses, 101 trims, 106 created
  0 failures (0 no memory)

The following is sample output from the `show buffers` command with no arguments, showing only buffer pool information for Huge buffers. This output shows a highest total of 184 Huge buffers created one hour, one minute, and 15 seconds before the command was issued.

Router# show buffers
Huge buffers, 65280 bytes (total 4, permanent 2, peak 184 @ 01:01:15):
  4 in free list (0 min, 4 max allowed)
  32521 hits, 143636 misses, 14668 trims, 14670 created
  143554 failures (0 no memory)
Router# show buffers Ethernet 0
Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
  16 in free list (0 min, 64 max allowed)
  48 hits, 0 fallbacks

16 max cache size, 16 in cache

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

Table 55: show buffers (Cisco IOS Software) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bufferelements</td>
<td>Small structures used as placeholders for buffers in internal operating system queues. Used when a buffer may need to be on more than one queue.</td>
</tr>
<tr>
<td>freelist</td>
<td>Total number of the currently unallocated buffer elements.</td>
</tr>
<tr>
<td>maxallowed</td>
<td>Maximum number of buffers that are available for allocation.</td>
</tr>
<tr>
<td>hits</td>
<td>Count of successful attempts to allocate a buffer when needed.</td>
</tr>
<tr>
<td>misses</td>
<td>Count of buffer allocation attempts that resulted in growing the buffer pool to allocate a buffer.</td>
</tr>
<tr>
<td>created</td>
<td>Count of new buffers created to satisfy buffer allocation attempts when the available buffers in the pool have already been allocated.</td>
</tr>
</tbody>
</table>

Public Buffer Pools

Small buffers | Buffers that are 104 bytes long. |
Middle buffers | Buffers that are 600 bytes long. |
Big buffers | Buffers that are 1524 bytes long. |
VeryBig buffers | Buffers that are 4520 bytes long. |
Large buffers | Buffers that are 5024 bytes long. |
Huge buffers | Buffers that are 18,024 bytes long. |

<p>| total     | Total number of this type of buffer. |
| permanent | Number of these buffers that are permanent. |
| peak      | Maximum number of buffers created (highest total) and the time when that peak occurred. Formats include weeks, days, hours, minutes, and seconds. Not all systems report a peak value, which means this field may not display in output. |
| freelist  | Number of available or unallocated buffers in that pool. |
| min       | Minimum number of free or unallocated buffers in the buffer pool. |
| maxallowed | Maximum number of free or unallocated buffers in the buffer pool. |
| hits      | Count of successful attempts to allocate a buffer when needed. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>misses</td>
<td>Count of buffer allocation attempts that resulted in growing the buffer pool in order to allocate a buffer.</td>
</tr>
<tr>
<td>trims</td>
<td>Count of buffers released to the system because they were not being used. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.</td>
</tr>
<tr>
<td>created</td>
<td>Count of new buffers created in response to misses. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.</td>
</tr>
</tbody>
</table>

### Interface Buffer Pools

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>Total number of this type of buffer.</td>
</tr>
<tr>
<td>permanent</td>
<td>Number of these buffers that are permanent.</td>
</tr>
<tr>
<td>free list</td>
<td>Number of available or unallocated buffers in that pool.</td>
</tr>
<tr>
<td>min</td>
<td>Minimum number of free or unallocated buffers in the buffer pool.</td>
</tr>
<tr>
<td>max allowed</td>
<td>Maximum number of free or unallocated buffers in the buffer pool.</td>
</tr>
<tr>
<td>hits</td>
<td>Count of successful attempts to allocate a buffer when needed.</td>
</tr>
<tr>
<td>fallbacks</td>
<td>Count of buffer allocation attempts that resulted in falling back to the public buffer pool that is the smallest pool at least as big as the interface buffer pool.</td>
</tr>
<tr>
<td>max cache size</td>
<td>Maximum number of buffers from the pool of that interface that can be in the buffer pool cache of that interface. Each interface buffer pool has its own cache. These are not additional to the permanent buffers; they come from the buffer pools of the interface. Some interfaces place all of their buffers from the interface pool into the cache. In this case, it is normal for the free list to display 0.</td>
</tr>
<tr>
<td>failures</td>
<td>Total number of times a buffer creation failed. The failure may have occurred because of a number of different reasons, such as low processor memory, low IOMEM, or no buffers in the pool when called from interrupt context.</td>
</tr>
<tr>
<td>no memory</td>
<td>Number of times there has been low memory during buffer creation. Low or no memory during buffer creation may not necessarily mean that buffer creation failed; memory can be obtained from an alternate resource such as a fallback pool.</td>
</tr>
</tbody>
</table>

**Cisco IOS Software Modularity**

The following is sample output from the `show buffers` command using a Cisco IOS Modularity image from Cisco IOS Release 12.2(18)SXF4 and later releases. Two new output fields were introduced—Public buffer heads and Temporary buffer heads—and are shown within comments in the following sample output.

```
Router# show buffers
Buffer elements:
    500 in free list (500 max allowed)
```
106586 hits, 0 misses, 0 created
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50, peak 54 @ 1d13h):
   49 in free list (20 min, 150 max allowed)
54486 hits, 0 misses, 4 trims, 4 created
   0 failures (0 no memory)
Middle buffers, 600 bytes (total 25, permanent 25, peak 27 @ 1d13h):
   25 in free list (10 min, 150 max allowed)
   20 hits, 0 misses, 2 trims, 2 created
   0 failures (0 no memory)
Big buffers, 1536 bytes (total 50, permanent 50):
   50 in free list (40 min, 150 max allowed)
   6 hits, 0 misses, 0 trims, 0 created
   0 failures (0 no memory)
VeryBig buffers, 4520 bytes (total 10, permanent 10):
   10 in free list (0 min, 100 max allowed)
   0 hits, 0 misses, 0 trims, 0 created
   0 failures (0 no memory)
Large buffers, 5024 bytes (total 0, permanent 0):
   0 in free list (0 min, 10 max allowed)
   0 hits, 0 misses, 0 trims, 0 created
   0 failures (0 no memory)
Huge buffers, 18024 bytes (total 1, permanent 0, peak 1 @ 1d13h):
   0 in free list (0 min, 4 max allowed)
   1 hits, 0 misses, 0 trims, 0 created
   0 failures (0 no memory)

! Start of Cisco IOS Software Modularity fields
Public buffer headers:
Header buffers, 880 bytes (total 1000, peak 142 @ 1d13h):
   864 in permanent free list
   142 hits, 0 misses
Temporary buffer headers:
Header buffers, 896 bytes (total 0):
   0 in free list
   0 hits, 0 misses, 0 trims, 0 created
   0 failures

! End of Cisco IOS Software Modularity fields
Interface buffer pools:
Logger Pool buffers, 600 bytes (total 150, permanent 150):
   150 in free list (150 min, 150 max allowed)
   22 hits, 0 misses

The table below describes the significant fields shown in the display that are different from the fields in the first table.

Table 56: show buffers (Cisco IOS Software Modularity) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Buffer Headers</td>
<td>Buffers that are 880 bytes long.</td>
</tr>
<tr>
<td>Header buffers</td>
<td>Total number of this type of buffer.</td>
</tr>
<tr>
<td>total</td>
<td>Number of available or unallocated permanent header buffers.</td>
</tr>
<tr>
<td>permanent free list</td>
<td>Count of successful attempts to allocate a header buffer when needed.</td>
</tr>
<tr>
<td>hits</td>
<td>Count of buffer allocation attempts that resulted in growing the buffer pool in order to allocate a buffer.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Temporary Buffer Headers | Buffers that are 896 bytes long.
Header buffers | Buffers that are 896 bytes long.
total | Total number of this type of buffer.
free list | Number of available or unallocated header buffers in that pool.
hits | Count of successful attempts to allocate a buffer when needed.
misses | Count of buffer allocation attempts that resulted in growing the buffer pool in order to allocate a buffer.
trims | Count of buffers released to the system because they were not being used. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.
created | Count of new buffers created in response to misses. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.
failures | Total number of allocation requests that have failed because no buffer was available for allocation; the datagram was lost. Such failures normally occur at interrupt level.

---

**Cisco Catalyst 4500e Series Switches running IOS XE software**

The following is sample output from the `show buffers` command on a Cisco Catalyst 4500e switch, using a Cisco IOS image from Cisco IOS XE Release 3.1.0.SG and later releases. PDS Public buffers and Packet information was added—and are shown within comments in the following sample output.

```
Switch#show buffers
PDS public buffers
Public buffer pools:
Packet buffer, 2048 bytes (total 1000, permanent 1000):
  1000 in free list (1000 max allowed)
Header pools:
Packet Header Memory, 0 bytes (total 0, permanent 0):
  0 in free list (0 max allowed)
Buffer Header Memory, 0 bytes (total 0, permanent 0):
  0 in free list (0 max allowed)
IOSd private buffers:
Buffer elements:
  354 in free list (500 max allowed)
  27134 hits, 0 misses, 500 created
```

```
Public buffer pools:
Small buffers, 104 bytes (total 134, permanent 50, peak 134 @ 01:04:39):
  134 in free list (20 min, 150 max allowed)
  2554 hits, 28 misses, 0 trims, 84 created
  0 failures (0 no memory)
Middle buffers, 600 bytes (total 52, permanent 25, peak 52 @ 01:04:39):
  52 in free list (10 min, 150 max allowed)
  61 hits, 9 misses, 0 trims, 27 created
  0 failures (0 no memory)
Big buffers, 1536 bytes (total 50, permanent 50):
```
50 in free list (5 min, 150 max allowed)
157 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

VeryBig buffers, 4520 bytes (total 10, permanent 10):
10 in free list (0 min, 100 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Large buffers, 5024 bytes (total 0, permanent 0):
0 in free list (0 min, 10 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Huge buffers, 18024 bytes (total 0, permanent 0):
0 in free list (0 min, 4 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Interface buffer pools:

CF Small buffers, 104 bytes (total 100, permanent 100):
100 in free list (100 min, 200 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

BIPC small buffers, 128 bytes (total 250, permanent 250):
250 in free list (250 min, 250 max allowed)
92 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

BIPC middle buffers, 600 bytes (total 300, permanent 300):
300 in free list (300 min, 300 max allowed)
36 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

CF Middle buffers, 600 bytes (total 100, permanent 100):
100 in free list (100 min, 200 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Syslog ED Pool buffers, 600 bytes (total 132, permanent 132):
131 in free list (132 min, 132 max allowed)
5 hits, 0 misses

CF Big buffers, 1536 bytes (total 25, permanent 25):
25 in free list (25 min, 50 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

BIPC buffers, 4096 bytes (total 2, permanent 2):
2 in free list (1 min, 8 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

IPC Emergency buffers, 4096 bytes (total 301, permanent 300, peak 302 @ 01:05:07):
301 in free list (300 min, 300 max allowed)
39 hits, 1 fallbacks, 66 trims, 67 created
0 failures (0 no memory)
0 max cache size, 0 in cache
0 hits in cache, 0 misses in cache

CF VeryBig buffers, 4520 bytes (total 2, permanent 2):
2 in free list (2 min, 4 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

CF Large buffers, 5024 bytes (total 1, permanent 1):
1 in free list (1 min, 2 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

BIPC Medium buffers, 16384 bytes (total 5, permanent 5):
5 in free list (5 min, 5 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

BIPC Large buffers, 65535 bytes (total 2, permanent 2):
2 in free list (2 min, 2 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

IPC small buffers, 128 bytes (total 250, permanent 250):
228 in free list (250 min, 250 max allowed)
124 hits, 0 fallbacks
0 max cache size, 0 in cache
0 hits in cache, 0 misses in cache

IPC middle buffers, 600 bytes (total 200, permanent 200):
200 in free list (200 min, 200 max allowed)
293 hits, 0 fallbacks
0 max cache size, 0 in cache
0 hits in cache, 0 misses in cache

IPC buffers, 4096 bytes (total 300, permanent 300):
298 in free list (300 min, 300 max allowed)
72 hits, 0 fallbacks
0 max cache size, 0 in cache
0 hits in cache, 0 misses in cache

IPC Medium buffers, 16384 bytes (total 30, permanent 30):
30 in free list (30 min, 30 max allowed)
100 hits, 0 fallbacks
0 max cache size, 0 in cache
0 hits in cache, 0 misses in cache

IPC Large buffers, 65535 bytes (total 13, permanent 13):
11 in free list (13 min, 13 max allowed)
19 hits, 0 misses
0 max cache size, 0 in cache
0 hits in cache, 0 misses in cache

Header pools:
Catalyst 4000 buffers, 0 bytes (total 14600, permanent 14600):
14600 in free list (0 min, 14601 max allowed)
14600 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Switch#

The following is sample shows how to run the **show buffers detailed** command on a Cisco Catalyst 4500e switch, using a Cisco IOS image from Cisco IOS XE Release 3.1.0.SG and later releases and the various keywords and arguments (Explained in the Syntax Description Table) available.

Switch#
Switch#show buffers ?
   detailed  Show detailed buffer statistics
   |      Output modifiers
   <cr>
Switch#show buffers detailed ?
   process  Show detailed process buffer info
Switch#show buffers detailed process ?
   iosd  IOSd Process
Switch#show buffers detailed process iosd ?
   address  Buffer at a given address
   all  All buffers
   assigned  Buffers in use
   failures  Buffer allocation failures
   free  Buffers available for use
   input-interface  Buffers assigned to an input interface
   old  Buffers older than one minute
   pool  Buffers in a specified pool
   |  Output modifiers
   <cr>
show c2600

To display information for troubleshooting the Cisco 2600 series router, use the show c2600 command in EXEC mode.

**show c2600**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 XA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The show c2600 command provides complex troubleshooting information that pertains to the platform’s shared references rather than to a specific interface.

**Examples**

The following is sample output from the show c2600 command:

```
Router# show c2600
C2600 Platform Information:
Interrupts:

Assigned Handlers...

<table>
<thead>
<tr>
<th>Vect</th>
<th>Handler</th>
<th># of Ints</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>801F224C</td>
<td>00000000</td>
<td>Xilinx bridge error interrupt</td>
</tr>
<tr>
<td>01</td>
<td>801DE768</td>
<td>0D3EE155</td>
<td>MPC860 TIMER INTERRUPT</td>
</tr>
<tr>
<td>02</td>
<td>801E94E0</td>
<td>0000119E</td>
<td>16552 Con/Aux Interrupt</td>
</tr>
<tr>
<td>04</td>
<td>801F0D94</td>
<td>00000000</td>
<td>PA Network Management Int Handler</td>
</tr>
<tr>
<td>05</td>
<td>801E6C34</td>
<td>00000000</td>
<td>Timebase Reference Interrupt</td>
</tr>
<tr>
<td>06</td>
<td>801F0DE4</td>
<td>00002C1A</td>
<td>PA Network IO Int Handler</td>
</tr>
<tr>
<td>07</td>
<td>801F0EA0</td>
<td>0000015D</td>
<td>MPC860 CPM INTERRUPT</td>
</tr>
<tr>
<td>14</td>
<td>801F224C</td>
<td>00000000</td>
<td>Xilinx bridge error interrupt</td>
</tr>
</tbody>
</table>

IOS Priority Masks...
Level 00 = [ EF020000 ]
Level 01 = [ EC020000 ]
Level 02 = [ E8020000 ]
Level 03 = [ E0020000 ]
Level 04 = [ E0020000 ]
Level 05 = [ E0020000 ]
Level 06 = [ C0020000 ]
Level 07 = [ 00000000 ]

SIU_IRQ_MASK = FFFFFFFF SIEN = EF02xxxx Current Level = 00
Spurious IRQs = 00000000 SIFEND = 0000xxxx

Interrupt Throttling:
Throttle Count = 00000000 Timer Count = 00000000
Netint usec = 00000000 Netint Mask usec = 000003E8
Active = 0 Configured = 0
Longest IRQ = 00000000

IDMA Status:
Requests = 00000349 Drops = 00000000
```
Complete = 00000349   Post Coalesce Frames = 00000349
Giant = 00000000
Available Blocks = 256/256

ISP Status:
Version string burned in chip: "A986122997"
New version after next program operation: "B018020998"
ISP family type: "2096"
ISP chip ID: 0x0013
Device is programmable

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

**Table 57: show c2600 Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interrupts</td>
<td>Denotes that the next section describes the status of the interrupt services.</td>
</tr>
<tr>
<td>Assigned Handlers</td>
<td>Denotes a subsection of the Interrupt section that displays data about the interrupt handlers.</td>
</tr>
<tr>
<td>Vect</td>
<td>The processor vector number.</td>
</tr>
<tr>
<td>Handler</td>
<td>The execution address of the handler assigned to this vector.</td>
</tr>
<tr>
<td># of Ints</td>
<td>The number of times this handler has been called.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the handler assigned to this vector.</td>
</tr>
<tr>
<td>IOS Priority Masks</td>
<td>Denotes the subsection of the Interrupt section that displays internal Cisco IOS priorities. Each item in this subsection indicates a Cisco IOS interrupt level and the bit mask used to mask out interrupt sources when that Cisco IOS level is being processed. Used exclusively for debugging.</td>
</tr>
<tr>
<td>SIU_IRQ_MASK</td>
<td>For engineering level debug only.</td>
</tr>
<tr>
<td>Spurious IRQs</td>
<td>For engineering level debug only.</td>
</tr>
<tr>
<td>Interrupt Throttling:</td>
<td>This subsection describes the behavior of the Interrupt Throttling mechanism on the platform.</td>
</tr>
<tr>
<td>Throttle Count</td>
<td>Number of times throttle has become active.</td>
</tr>
<tr>
<td>Timer Count</td>
<td>Number of times throttle has deactivated because the maximum masked out time for network interrupt level has been reached.</td>
</tr>
<tr>
<td>Netint usec</td>
<td>Maximum time network level is allowed to run (in microseconds).</td>
</tr>
<tr>
<td>Netint Mask usec</td>
<td>Maximum time network level interrupt is masked out to allow process level code to run (in microseconds).</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates that the network level interrupt is masked or that the router is in interrupt throttle state.</td>
</tr>
<tr>
<td>Configured</td>
<td>Indicates that throttling is enabled or configured when set to 1.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Longest IRQ</td>
<td>Duration of longest network level interrupt (in microseconds).</td>
</tr>
<tr>
<td>IDMA Status</td>
<td>Monitors the activity of the Internal Direct Memory Access (IDMA) hardware and software. Used to coalesce packets (turn particularized packets into non particularized packets) for transfer to the process level switching mechanism.</td>
</tr>
<tr>
<td>Requests</td>
<td>Number of times the IDMA engine is asked to coalesce a packet.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of times the coalescing operation was aborted.</td>
</tr>
<tr>
<td>Complete</td>
<td>Number of times the operation was successful.</td>
</tr>
<tr>
<td>Post Coalesce Frames</td>
<td>Number of Frames completed post coalesce processing.</td>
</tr>
<tr>
<td>Giant</td>
<td>Number of packets too large to coalesce.</td>
</tr>
<tr>
<td>Available Blocks</td>
<td>Indicates the status of the request queue, in the format N/M where N is the number of empty slots in queue and M is the total number of slots; for example, 2/256 indicates that the queue has 256 entries and can accept two more requests before it is full.</td>
</tr>
<tr>
<td>ISP Status</td>
<td>Provides status of In-System-Programmable (ISP) hardware.</td>
</tr>
<tr>
<td>Version string burned in chip</td>
<td>Current version of ISP hardware.</td>
</tr>
<tr>
<td>New version after next program operation</td>
<td>Version of ISP hardware after next ISP programming operation.</td>
</tr>
<tr>
<td>ISP family type</td>
<td>Device family number of ISP hardware.</td>
</tr>
<tr>
<td>ISP chip ID</td>
<td>Internal ID of ISP hardware as designated by the chip manufacturer.</td>
</tr>
<tr>
<td>Device is programmable</td>
<td>“Yes” or “No.” Indicates if an ISP operation is possible on this board.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show context</td>
<td>Displays information stored in NVRAM when the router crashes.</td>
</tr>
</tbody>
</table>

### show c7200

To display information about the CPU and midplane for Cisco 7200 series routers, use the `show c7200` command in EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC
show catalyst6000

To display the information about the chassis, use the **show catalyst6000** command in user EXEC or privileged EXEC mode.

```
show catalyst6000 {all|chassis-mac-address|switching-clock|traffic-meter}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays the MAC-address ranges and the current and peak traffic-meter reading.</td>
</tr>
<tr>
<td>chassis-mac-address</td>
<td>Displays the MAC-address range.</td>
</tr>
<tr>
<td>switching-clock</td>
<td>Displays the failure recovery mode of the switching clock.</td>
</tr>
<tr>
<td>traffic-meter</td>
<td>Displays the percentage of the backplane (shared bus) utilization.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is **all**
show catalyst6000

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>The output of the <strong>show catalyst6000 traffic-meter</strong> command was changed to include traffic monitor status information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you enter the **switching-clock** keywords, the output displays whether switching of the redundant clock sources on the backplane is allowed if the active clock source fails.

There are either 64 or 1024 MAC addresses that are available to support the software features. You can enter the **show catalyst6000 chassis-mac-address** command to display the MAC-address range on your chassis.

In Cisco IOS Release 12.2(33)SXI and later releases, the traffic monitor status information is displayed in the output. In earlier releases, only the current and peak traffic-meter readings are displayed.

**Examples**

This example shows how to display the MAC-address ranges and the current and peak traffic-meter readings:

```text
Router>
show catalyst6000 all
chassis MAC addresses: 64 addresses from 0001.6441.60c0 to 0001.6441.60ff
  traffic meter = 0% Never cleared
  peak = 0% reached at 08:14:38 UTC Wed Mar 19 2003

switching-clock: clock switchover and system reset is allowed
```

Router>

This example shows how to display the MAC-address ranges:

```text
Router#
show catalyst6000 chassis-mac-address
chassis MAC addresses: 1024 addresses from 00d0.004c.1800 to 00d0.004c.1c00
```

Router#

The following example shows how to display the current and peak traffic-meter readings and the traffic monitor status:

```text
Router>
show catalyst6000 traffic-meter
traffic meter = 0% Never cleared
  peak = 0% reached at 10:54:49 UTC Wed Mar 19 2008
  Traffic Utilization Monitor Status --------
          State | Interval | Threshold | MsgCount | LastMsgTime
  Backplane Off       60s         80%          0          --
  Fpoe#0 In Off       60s         80%          0          --
        out Off       60s         80%          0          --
  Fpoe#1 In Off       60s         80%          0          --
        out Off       60s         80%          0          --
  Fpoe#2 In Off       60s         80%          0          --
```

---
show cls

To display the current status of all Cisco link services (CLS) sessions on the router, use the `show cls` command in EXEC mode.

```
show cls [brief]
```

**Syntax Description**

- **brief** (Optional) Displays a brief version of the output.

**Command Default**

Without the brief keyword, displays complete output.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced in a release prior to Cisco IOS Release 11.0.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

This example shows how to display the failure recovery mode of the switching clock:

```
Router> show catalyst6000 switching-clock
switching-clock: clock switchover and system reset is allowed
Router>
```
Usage Guidelines

The Cisco link service (CLS) is used as the interface between data link users (DLUs), such as DLSw, LAN Network Manager (LNM), downstream physical unit (DSPU), and SNASw, and their corresponding data link circuits (DLCs) such as Logic Link Control (LLC), VDLC, and Qualified Logic Link Control (QLLC). Each DLU registers a particular service access point (SAP) with CLS, and establishes circuits through CLS over the DLC.

The show cls command displays the SAP values associated with the DLU and the circuits established through CLS.

For further information about CLS, use the Release 12.2 Cisco IOS Bridging and IBM Networking Configuration Guide.

Examples

The following is sample output from the show cls command:

```
IBD-4500B# show cls
DLU user:SNASW
   SSap:0x04  VDLC VDLC650
   DTE:1234.4000.0001 1234.4000.0002 04 04
   T1 timer:0  T2 timer:0  Inact timer:0
   max out:0  max in:0  retry count:10
   XID retry:10  XID timer:5000  I-Frame:0
   flow:0  DataIndQ:0  DataReqQ:0
DLU user:DLSWDLUPEER
DLU user:DLSWDLU
   Bridging  VDLC VDLC1000
   Bridging  VDLC VDLC650
```

The following is sample output from the show cls brief command:

```
IBD-4500B# show cls brief
DLU user:SNASW
   SSap:0x04  VDLC VDLC650
   DTE:1234.4000.0001 1234.4000.0002 04 04
DLU user:DLSWDLUPEER
DLU user:DLSWDLU
   Bridging  VDLC VDLC1000
   Bridging  VDLC VDLC650

Bridging VDLC VDLC650
```

The examples show two DLUs--SNASw and DLSw--active in the router. SNASw uses a SAP value of 0x04, and the associated DLC port is VDLC650. SNASw has a circuit established between MAC addresses 1234.4000.0001 and 1234.4000.0002 using source and destination SAPs 04 and 04. DLSw is a bridging protocol and uses VDLC1000 and VDLC650 ports. There are no circuits in place at this time.

In the output from the show cls command (without the brief argument), the values of timers and counters applicable to this circuit are displayed.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stun peer-name</td>
<td>Enables STUN for an IP address and uses Cisco Link Services (CLS) to access the Frame Relay network.</td>
</tr>
</tbody>
</table>
**show config id**

The configuration change tracking identifier (CTID) assigns a version number to each saved version of the running-config file. To display output about the versions, use the `show config id` command in privileged EXEC mode.

```
show config id [detail]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>(Optional) Expands the output of the command to include the ID of the last user to make a configuration change and the process in which the changes were made.</td>
</tr>
</tbody>
</table>

### Command Default

This command is disabled by default. If this command is not entered, the management system has to query the device for the current running-config file and then compare the results to the last known configuration to determine if a change has been made.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This configuration infrastructure command assigns a version number that is updated every time the running-config file is changed. This version number is called the configuration change tracking identifier or CTID. The CTID can be used to compare configuration files to track configuration changes and take appropriate actions (for example, a configuration rollback). Config Logger can also use the CTID to determine if there have been any changes to the running-config file.

CTID makes the management system more efficient by presenting information that indicates a change has been made to the running-config file. Without CTID, the management system has to query the device for the current running-config file and then compare the results to the last known configuration to determine if a change has been made.

### Examples

The following example shows that the current running-config file is version 4 and that this file was saved on June 15, 2006 at 7:572 seconds after 3:02 p.m.:

```
Device# show config id
version:4 time:2006-06-15T15:02:07.572Z
```

The following example shows that the current running-config file is version 9 and that this file was last saved on June 18, 2006 at 34.431 seconds after 6:34 p.m. The file was saved by the system and changed from Init:
Device# show config id detail

Configuration version : 9
Last change time : 2006-06-18T18:34:34.431Z
Changed by user : system
Changed from process : Init

Field descriptions are self-explanatory.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>Copies the current running-config file (source) to the startup-config file (destination).</td>
</tr>
<tr>
<td></td>
<td>show running-config</td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or virtual-circuit class.</td>
</tr>
</tbody>
</table>

**show configuration id**

To display output about configuration versions, use the `show configuration id` command in privileged EXEC mode.

`show configuration id [detail]`

**Syntax Description**

| Syntax Description | detail | (Optional) Expands the output of the command to include the ID of the last user to make a configuration change and the process in which the changes were made. |

**Command Default**

This command is disabled by default. If this command is not entered, the management system has to query the device for the current running-config file and then compare the results to the last known configuration to determine if a change has been made.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This configuration infrastructure command assigns a version number that is updated every time the running-config file is changed. This version number is called the configuration change tracking identifier (CTID). The CTID assigns a version number to each saved version of the running-config file. The CTID can be used to compare configuration files to track configuration changes and take appropriate actions (for example,
a configuration rollback). Config Logger can also use the CTID to determine if there have been any changes to the running-config file.

CTID makes the management system more efficient by presenting information that indicates a change has been made to the running-config file. Without CTID, the management system has to query the device for the current running-config file and then compare the results to the last known configuration to determine if a change has been made.

Examples

The following example shows that the current running-config file is version 4 and that this file was saved on June 15, 2006 at 7.572 seconds after 3:02 p.m.:

Router# show configuration id
version:4 time:2006-06-15T15:02:07.572Z

The following example shows that the current running-config file is version 9 and that this file was last saved on June 18, 2006 at 34.431 seconds after 6:34 p.m. The file was saved by the system and changed from Init. The field descriptions are self-explanatory.

Router# show configuration id detail

Configuration version : 9
Last change time : 2006-06-18T18:34:34.431Z
Changed by user : system
Changed from process : Init

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>Copies the current running-config file (source) to the startup-config file (destination).</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or virtual-circuit class.</td>
</tr>
</tbody>
</table>

show configuration lock

To display information about the lock status of the running configuration file during a configuration replace operation, use the **show configuration lock** command in privileged EXEC mode.

**Syntax Description**

- This command has no arguments or keywords.

**Command Modes**

- Privileged EXEC(

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(25)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
## Examples

The following is sample output from the `show configuration lock` command when the running configuration file is locked by another user.


Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# configuration mode exclusive ?
auto  Lock configuration mode automatically
manual  Lock configuration mode on-demand
Device(config)# configuration mode exclusive auto

Device(config)# end
Device# show running-config
| include configuration
configuration mode exclusive auto
Device# configure terminal

!---------- Acquires the lock
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# show configuration lock

Parser Configure Lock
------------------------
Owner PID : 3
User : unknown
TTY : 0
Type : EXCLUSIVE
State : LOCKED
Class : EXPOSED
Count : 1
Pending Requests : 0

### Release | Modification
--- | ---
12.3(14)T | This command was integrated into Cisco IOS Release 12.3(14)T. The output of this command was updated to display the configuration locking class.
12.0(31)S | The command output was enhanced.
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)SB2 | This command was implemented on the Cisco 10000 series.
12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
Cisco IOS XE Release 3.9S | This command was integrated into Cisco IOS XE Release 3.9S.
User debug info : configure terminal
Device(config)#
Device(config)# end
! <------------ Releases the lock

The following is sample output from the `show configuration lock` command when the running
configuration file is not locked by another user.

Device# `show configuration lock`

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :

Cisco IOS Release 12.0(31)S, 12.2(33)SRA, and Later Releases

Device# `show configuration lock`
Parser Configure Lock
---------------------
Owner PID : 3
User : unknown
TTY : 0
Type : EXCLUSIVE
State : LOCKED
Class : EXPOSED
Count : 1
Pending Requests : 0
User debug info : configure terminal
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 6
Lock Expiration timer (in Sec) : 593

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

**Table 58: show configuration lock Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner PID</td>
<td>Process identifier (PID) of the process that owns the lock.</td>
</tr>
<tr>
<td>User</td>
<td>Owner’s username.</td>
</tr>
<tr>
<td>TTY</td>
<td>Owner’s terminal number.</td>
</tr>
<tr>
<td>Type</td>
<td>Lock type (EXCLUSIVE/COUNTER/NO LOCK).</td>
</tr>
<tr>
<td>State</td>
<td>State of the lock (FREE/LOCKED).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Class</td>
<td>Classification of users of the lock (EXPOSED/ROLLBACK). Processes other than ROLLBACK belong to the EXPOSED class.</td>
</tr>
<tr>
<td>Count</td>
<td>In the case of a counter lock, total number of processes holding the lock.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>Total number of processes blocked by the lock.</td>
</tr>
<tr>
<td>User debug info</td>
<td>Any string given by the process (used for debugging only).</td>
</tr>
<tr>
<td>Session idle state</td>
<td>Indicates whether the user in an access session locking session is idle. Displays TRUE or FALSE.</td>
</tr>
<tr>
<td>No of exec cmds getting executed</td>
<td>Total number of EXEC commands (show and clear) being executed simultaneously from different sessions.</td>
</tr>
<tr>
<td>No of exec cmds blocked</td>
<td>Total number of EXEC commands (show and clear) waiting for the configuration command (running from the access session locking session) to complete its execution.</td>
</tr>
<tr>
<td>Config wait for show completion</td>
<td>Indicates whether a configuration command executed in an access session locking session is waiting for the completion of the show command being executed simultaneously from a different session. Displays TRUE or FALSE.</td>
</tr>
<tr>
<td>Remote ip address</td>
<td>IP address of the terminal from which the user telneted to the router.</td>
</tr>
<tr>
<td>Lock active time (in Sec)</td>
<td>Amount of time, in seconds, that elapsed since the lock was acquired.</td>
</tr>
<tr>
<td>Lock Expiration timer (in Sec)</td>
<td>The amount of time, in seconds, that expires before the lock is automatically released.</td>
</tr>
</tbody>
</table>

The following example shows how to configure the configuration file for single user auto configuration mode (using the configuration mode exclusive auto command). Use the configure terminal command to enter global configuration mode and lock the configuration mode exclusively. Once the Cisco IOS configuration mode is locked exclusively, you can verify the lock using the show configuration lock command.

```
Device# configure terminal
Device(config)# configuration mode exclusive auto
Device(config)# end
Device# configure terminal
Device(config)# show configuration lock
Parser Configure Lock
Owner PID     : 10
User          : User1
TTY           : 3
Type          : EXCLUSIVE
State         : LOCKED
Class         : Exposed
Count         : 0
Pending Requests : 0
User debug info : 0
```
show context

To display information stored in NVRAM when an unexpected system reload (system exception) occurs, use the `show context` command in user EXEC or privileged EXEC mode.

```
show context [{summary|all|slot  slot-number [crash-index] [all] [debug]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays a summary of all the crashes recorded.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all crashes for all the slots. When optionally used with the <code>slot</code> keyword, displays crash information for the specified slot.</td>
</tr>
<tr>
<td>slot</td>
<td>Displays information for a particular line card. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008. The index number allows you to look at previous crash contexts. Contexts from the last 24 line card crashes are saved on the GRP card. If the GRP reboots, the last 24 line card crash contexts are lost. For example, <code>show context slot 3 2</code> shows the second most recent crash for line card in slot 3. Index numbers are displayed by the <code>show context summary</code> command.</td>
</tr>
<tr>
<td>crash-index</td>
<td></td>
</tr>
<tr>
<td>debug</td>
<td>(Optional) Displays crash information as a hex record dump in addition to one of the options listed.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2 GS</td>
<td>The <code>slot  slot-number [crash-index] [all] [debug]</code> syntax was added for Cisco 12000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The display from the `show context` command includes the following information:

- Reason for the system reboot
- Stack trace
- Software version
• The signal number, code, and router uptime information
• All the register contents at the time of the crash

**Note**

This command is primarily for use by Cisco technical support representatives for analyzing unexpected system reloads.

Output for this command will vary by platform. Context information is specific to processors and architectures. For example, context information for the Cisco 2600 series router differs from that for other router types because the Cisco 2600 runs with an M860 processor.

**Examples**

The following is sample output from the `show context` command following a system failure:

```
Router> show context
System was restarted by error - a Software forced crash, PC 0x60189354
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Image text-base: 0x60010900, data-base: 0x6073E000
Stack trace from system failure:
FP: 0x60A8E798, RA: 0x60189354
FP: 0x60A8E798, RA: 0x601853CC
FP: 0x60A8E7F8, RA: 0x60111AB9C
FP: 0x60A8E828, RA: 0x601706CC
FP: 0x60A8E878, RA: 0x60116340
FP: 0x60A8E900, RA: 0x6011632C
Fault History Buffer:
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Signal = 23, Code = 0x24, Uptime 00:04:19
$0 : 00000000, AT : 60930120, v0 : 00000032, v1 : 00000120
a0 : 60170110, a1 : 6097F22C, a2 : 00000000, a3 : 00000000
a0 : 60170110, a1 : 6097F22C, a2 : 00000000, a3 : 00000000
 FP: 0x60A8E798, RA: 0x60189354
 t0 : 60A02A0, t1 : 8000FD80, t2 : 34008F00, t3 : FFFF00FF
 t4 : 00000000, t5 : 3848D024, t6 : 00000000, t7 : 11010132
 a0 : 00000006, a1 : 607A25F8, a2 : 00000001, a3 : 00000000
 a4 : 00000000, a5 : 00000000, a6 : 00000000, a7 : 6097F755
 t8 : 600FABBC, t9 : 00000000, k0 : 30408401, k1 : 30410000
 gp : 608B9860, sp : 60AEA798, s8 : 00000000, ra : 601853CC
 EPC : 60189354, SREG : 3400EF03, Cause : 00000024
Router>
```

The following is sample output from the `show context summary` command on a Cisco 12012 router. The `show context summary` command displays a summary of all the crashes recorded for each slot (line card).

```
Router# show context summary
CRASH INFO SUMMARY
 Slot 0 : 0 crashes
 Slot 1 : 0 crashes
 Slot 2 : 0 crashes
 Slot 3 : 0 crashes
 Slot 4 : 0 crashes
 Slot 5 : 0 crashes
 Slot 6 : 0 crashes
 Slot 7 : 2 crashes
  1 - crash at 18:06:41 UTC Tue Nov 5 1996
```
The following is sample output from the `show context` command following an unexpected system reload on a Cisco 2600 series router.

```
router# show context
S/W Version: Cisco IOS Software
Cisco IOS (tm) c2600 Software (c2600-JS-M), Released Version 11.3(19980115:184921)
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Thu 15-Jan-98 13:49 by mmagno
Exception occurred at: 00:02:26 UTC Mon Mar 1 1993
Exception type: Data TLB Miss (0x1200)
CPU Register Context:
PC = 0x80109964 MSR = 0x00000030 CR = 0x55FFFFD3 LR = 0x80109958
CTR = 0x80109964 XER = 0x00000000 CR = 0x55FFFFD3 LR = 0x80109958
DEC = 0x7FFFDFFCA THB = 0x00000000 TBL = 0x15433FCF IMM = 0x68010102
R0 = 0x80000000 R1 = 0x80E815D0 R2 = 0x80000000 R3 = 0x00000000
R4 = 0x80E80B0C R5 = 0x80E80B00 R6 = 0x00000000 R7 = 0x80109958
R8 = 0x00000000 R9 = 0x00000000 R10 = 0x00000000 R11 = 0x00000000
R12 = 0x00000000 R13 = 0x00000000 R14 = 0x00000000 R15 = 0x00000000
R16 = 0x00000000 R17 = 0x00000000 R18 = 0x00000000 R19 = 0x00000000
R20 = 0x00000000 R21 = 0x00000000 R22 = 0x00000000 R23 = 0x00000000
R24 = 0x00000000 R25 = 0x00000000 R26 = 0x00000000 R27 = 0x00000000
R28 = 0x00000000 R29 = 0x00000000 R30 = 0x00000000 R31 = 0x00000000
Stack trace:
Frame 00: SP = 0x80E80B00 PC = 0x80109958
Frame 01: SP = 0x80E80B00 PC = 0x8010A720
Frame 02: SP = 0x80E80C40 PC = 0x80271010
Frame 03: SP = 0x80E80C50 PC = 0x8025EE64
Frame 04: SP = 0x80E80E548 PC = 0x8026702C
Frame 05: SP = 0x80E80E558 PC = 0x8026702C
```

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

```
Table 59: show context Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S/W Version</td>
<td>Standard Cisco IOS version string as displayed.</td>
</tr>
<tr>
<td>Exception occurred at</td>
<td>Router real time when exception occurred. The router must have the clock time properly configured for this to be accurate.</td>
</tr>
<tr>
<td>Exception type</td>
<td>Technical reason for exception. For engineering analysis.</td>
</tr>
<tr>
<td>CPU Register Context</td>
<td>Technical processor state information. For engineering analysis.</td>
</tr>
<tr>
<td>Stack trace</td>
<td>Technical processor state information. For engineering analysis.</td>
</tr>
</tbody>
</table>
```

Related Commands

```
Command  | Description                                      |
----------|-------------------------------------------------|
show processes | Displays information about the active processes. |
show stacks    | Monitors the stack usage of processes and interrupt routines. |
```
show controllers (GRP image)

To display information that is specific to the hardware, use the `show controllers` command in privileged EXEC mode.

```
show controllers [{atm slot-number} clock|csar register|cs-c-fpga|dp83800|fab-clk|fia [register]|pos [slot-number] [details]|queues [slot-number]|sca|xbar]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>atm slot-number</code></td>
<td>(Optional) Displays the ATM controllers. Number is slot-number/ port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.</td>
</tr>
<tr>
<td><code>clock</code></td>
<td>(Optional) Displays the clock card configuration.</td>
</tr>
<tr>
<td><code>csar [register]</code></td>
<td>(Optional) Displays the Cisco Cell Segmentation and Reassembly (CSAR) information. CSAR is the name of the chip on the card that handles traffic between the GRP and the switch fabric interface ASICs.</td>
</tr>
<tr>
<td><code>cs-c-fpga</code></td>
<td>(Optional) Displays the clock and scheduler card register information in the field programmable gate array (FPGA).</td>
</tr>
<tr>
<td><code>dp83800</code></td>
<td>(Optional) Displays the Ethernet information on the GRP card.</td>
</tr>
<tr>
<td><code>fab-clk</code></td>
<td>(Optional) Display the switch fabric clock register information. The switch fabric clock FPGA is a chip that monitors the incoming fabric clock generated by the switch fabric. This clock is needed by each card connecting to the switch fabric to properly communicate with it. Two switch fabric clocks arrive at each card; only one can be used. The FPGA monitors both clocks and selects which one to use if only one of them is running.</td>
</tr>
<tr>
<td><code>fia register</code></td>
<td>(Optional) Displays the fabric interface ASIC information and optionally displays the register information.</td>
</tr>
<tr>
<td><code>pos [slot-number] [details]</code></td>
<td>(Optional) Displays the POS framer state and optionally displays all the details for the interface. Number is slot-number/ port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.</td>
</tr>
<tr>
<td><code>queues [slot-number]</code></td>
<td>(Optional) Displays the SDRAM buffer carve information and optionally displays the information for a specific line card. The SDRAM buffer carve information displayed is suggested carve information from the GRP card to the line card. Line cards might change the shown percentages based on SDRAM available. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008.</td>
</tr>
<tr>
<td><code>sca</code></td>
<td>(Optional) Displays the SCA register information. The SCA is an ASIC that arbitrates among the line cards requests to use the switch fabric.</td>
</tr>
<tr>
<td><code>xbar</code></td>
<td>(Optional) Displays the crossbar register information. The XBAR is an ASIC that switches the data as it passes through the switch fabric.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 GS</td>
<td>This command was introduced to support the Cisco 12000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This information provided by this command is intended for use only by technical support representatives in analyzing system failures in the field.

Examples

The following is sample output from the `show controllers pos` command for a Cisco 12012:

```
Router# show controllers pos 7/0
POS7/0
SECTION
  LOF = 2  LOS = 0  BIP(B1) = 5889
  Active Alarms: None
LINE
  AIS = 2  RDI = 2  FEBE = 146  BIP(B2) = 2106453
  Active Alarms: None
PATH
  AIS = 2  RDI = 4  FEBE = 63  BIP(B3) = 3216
  LOF = 0  PSE = 8  NSE = 3  NEWPTR = 2
  Active Alarms: None
APS
  COAPS = 3  PSBF = 2
  State: PSBF_state = False
  Rx(K1/K2): F0/15  Tx(K1/K2): 00/00
  S1S0 = 00, C2 = 64
PATH TRACE BUFFER : STABLE
  Remote hostname : GSR-C
  Remote interface: POS10/0
  Remote IP addr : 10.201.101.2
  Remote Rx(K1/K2): F0/15  Tx(K1/K2): 00/00
Router#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controllers</td>
<td>Resets the T1 or E1 controller.</td>
</tr>
<tr>
<td>show controllers (line card image)</td>
<td>Displays information that is specific to the hardware on a line card.</td>
</tr>
</tbody>
</table>

**show controllers (line card image)**

To display information that is specific to the hardware on a line card, use the `attach` command in privileged EXEC mode to connect to the line card and then use the `show controllers` command in privileged EXEC mode or the `execute-on` command in privileged EXEC mode.

```
show controllers atm [[port-number] [{all|sar|summary}]]
show controllers fia [register]
show controllers {frfab|ofab} {bma|microcode|ms-inst|register}|qelem start-queue-element
show controllers io
show controllers l3
```
show controllers pos \{framers|queues|registers\}rxsram \(port-number\) queue-start-address \(queue-length\)\[txsram \(port-number\) queue-start-address \(queue-length\)\]
show controllers events \([\{clear|punt-sniff \{\{none|word1|word2\}\}\}punt-verbose \{all\}]\)

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>atm</code></td>
<td>Displays the ATM controller information.</td>
</tr>
<tr>
<td><code>port-number</code></td>
<td>(Optional) Displays request for the physical interface on the ATM card. The range of choices is from 0 to 3.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Lists all details.</td>
</tr>
<tr>
<td><code>sar</code></td>
<td>(Optional) Lists SAR interactive command.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Lists SAR status summary.</td>
</tr>
<tr>
<td><code>fia</code></td>
<td>Displays the fabric interface ASIC information.</td>
</tr>
<tr>
<td><code>register</code></td>
<td>(Optional) Displays the register information.</td>
</tr>
<tr>
<td><code>frfab</code></td>
<td>(Optional) Displays the &quot;from&quot; (transmit) fabric information.</td>
</tr>
<tr>
<td><code>tofab</code></td>
<td>(Optional) Displays the &quot;to&quot; (receive) fabric information.</td>
</tr>
<tr>
<td><code>bma</code></td>
<td>For the <code>frfab</code> or <code>tofab</code> keywords, displays microcode, micro sequencer, or register information for the silicon queuing engine (SQE), also known as the buffer management ASIC (BMA).</td>
</tr>
<tr>
<td><code>microcode</code></td>
<td>Displays SQE information for the microcode bundled in the line card and currently running version.</td>
</tr>
<tr>
<td><code>mis-inst</code></td>
<td>Displays SQE information for the micro sequencer instruction.</td>
</tr>
<tr>
<td><code>register</code></td>
<td>Displays silicon queuing engine (SQE) information for the register.</td>
</tr>
<tr>
<td><code>qelem</code></td>
<td>For the <code>frfab</code> or <code>tofab</code> keywords, displays the SDRAM buffer pool queue element summary information.</td>
</tr>
<tr>
<td><code>start-queue-element</code></td>
<td>Specifies the start queue element number from 0 to 65535.</td>
</tr>
<tr>
<td><code>end-queue-element</code></td>
<td>(Optional) Specifies the end queue element number from 0 to 65535.</td>
</tr>
<tr>
<td><code>qnum</code></td>
<td>For the <code>frfab</code> or <code>tofab</code> keywords, displays the SDRAM buffer pool queue detail information.</td>
</tr>
<tr>
<td><code>start-queue-number</code></td>
<td>Specifies the start free queue number (from 0 to 127).</td>
</tr>
<tr>
<td><code>end-queue-number</code></td>
<td>(Optional) Specifies the end free queue number (from 0 to 127).</td>
</tr>
<tr>
<td><code>queues</code></td>
<td>For the <code>frfab</code> or <code>tofab</code> keywords, displays the SDRAM buffer pool information.</td>
</tr>
<tr>
<td><code>statistics</code></td>
<td>For the <code>frfab</code> or <code>tofab</code> keywords, displays the BMA counters.</td>
</tr>
<tr>
<td><code>io</code></td>
<td>Displays input/output registers.</td>
</tr>
<tr>
<td><code>l3</code></td>
<td>Displays Layer 3 ASIC information.</td>
</tr>
<tr>
<td><strong>pos</strong></td>
<td>Displays packet-over-sonic (POS) information for framer registers, framer queues, and ASIC registers.</td>
</tr>
<tr>
<td><strong>framers</strong></td>
<td>Displays the POS framer registers.</td>
</tr>
<tr>
<td><strong>queues</strong></td>
<td>Displays the POS framer queue information.</td>
</tr>
<tr>
<td><strong>registers</strong></td>
<td>Displays the ASIC registers.</td>
</tr>
<tr>
<td><strong>rxsram</strong></td>
<td>Displays the receive queue SRAM.</td>
</tr>
<tr>
<td><strong>port-number</strong></td>
<td>Specifies a port number (valid range is from 0 to 3).</td>
</tr>
<tr>
<td><strong>queue-start-address</strong></td>
<td>Specifies the queue SRAM logical starting address.</td>
</tr>
<tr>
<td><strong>queue-length</strong></td>
<td>(Optional) Specifies the queue SRAM length.</td>
</tr>
<tr>
<td><strong>txsram</strong></td>
<td>Displays the transmit queue SRAM.</td>
</tr>
<tr>
<td><strong>events</strong></td>
<td>Displays the line card counter information of events generated from line card.</td>
</tr>
<tr>
<td><strong>clear</strong></td>
<td>(Optional) Clears all the line card event counter output details that are displayed using the commands: <code>show controllers events</code>, <code>show controllers events punt-verbose</code>, and <code>show controllers events punt-sniff</code>.</td>
</tr>
<tr>
<td><strong>punt-sniff</strong></td>
<td>(Optional) Sniffs the packets sent to route processor from line card by specifying the word and location.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Punt sniff is enabled only if one of the word is configured.</td>
</tr>
<tr>
<td><strong>none</strong></td>
<td>(Optional) Clears the attributes and packets to be sniffed from route processor and resets the counters to zero.</td>
</tr>
<tr>
<td><strong>word1</strong></td>
<td>(Optional) Sniffs packets sent to the route processor for the specified hexa decimal value of word1. Location of the word is optional.</td>
</tr>
<tr>
<td><strong>word2</strong></td>
<td>(Optional) Sniffs packets sent to the route processor matching the specified hexa decimal value of word2. Location of the word is optional.</td>
</tr>
<tr>
<td><strong>punt-verbose</strong></td>
<td>(Optional) Displays application-wise packets punt to route processor (RP) from line card (LC). Displays non-zero punt counters if the command is executed without the all keyword.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>(Optional) Displays zero and non-zero punt counters of packets punt to RP from LC. The all keyword is used along with the command <code>show controllers events punt-verbose all</code>.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 GS</td>
<td>This command was added to support the Cisco 12000 series Gigabit Switch Routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.2(31)SB</td>
<td>This command was integrated in Cisco IOS Release 12.2(31)SB.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command’ behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.</td>
</tr>
<tr>
<td>12.0(33)S</td>
<td>The keywords <strong>punt-sniff</strong> and <strong>punt-verbose</strong> were added in the command <strong>show controllers events</strong> for the Cisco 12000 Series Routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This information displayed by this command is of use only to technical support representatives in analyzing unexpected system failures in the field. It is documented here in case you need to provide the displayed statistics to an technical support engineer.

**Cisco 10000 Series Router Usage Guidelines**

In releases prior to Cisco IOS Release 12.2(33)SB, when you configure the t1 loopback remote command on the local router, the command also displays in the running-config file of the far-end router. This is due to the route processor (RP) updating an incorrect parameter when it receives the loopback event message from the line card for loopback requests from the far end.

In Cisco IOS Release 12.2(33)SB, the RP updates the correct parameter and the show controllers command correctly displays the loopback CLI commands applied on the local end and displays the loopback events and status received from the line card in response to loopback requests from the far end.

This change in behavior affects the following line cards and is documented in the CSCsm84447 caveat:

- 4-port channelized STM1
- 1-port channelized OC-12
- 6-port channelized T3
- 4-port half-height channelized T3

In Cisco IOS Release 12.2(33)SB, the output from the show controller command includes line code information for the 6-port channelized T3 line card and the 8-port E3/DS3 line card. However, because SONET line cards do not have a direct physical link at the T3 or E3 level, the output from the show controller t3 command does not include line code information.

In Cisco IOS Release 12.2(31)SB, the output from the show controller command displays line code information. The output of the show controller t3 command for SONET-based T3 also includes line code information.

**Cisco 12000 Series Router Usage Guidelines**

The packets processed by a line card are either sent to a route processor or a line card in the form of Cisco cells. To track the packets sent to a route processor from a line card is essential for troubleshooting. The keywords **punt-sniff** and **punt-verbose** have been added for the command **show controllers events** to identify the packets sent to RP from LC.

By default, the feature is enabled and packets punt to route processor are displayed using the command **show controllers events punt-verbose**. To view all the zero and non-zero punt counters use the command **show controllers events punt-verbose all**.

To clear all the line card events and counters including resetting the packets to be sniffed to zero, executing the command **show controllers events clear**.
Packets sent to route processor from line card can be sniffed by specifying the hexa-decimal value of the word. Packets can only be sniffed if the word along with the hexa-decimal value is specified. Specifying the location of the word, sniffs packets from the particular location. To reset the counters of packets to be sniffed to zero, execute the command `show controllers events punt-sniff none`.

For example, use the command `show controllers events punt-sniff word1 0x60000000` to sniff packets punt to RP with the hexa-decimal value 0x60000000. As the location is not specified, it searches the entire buffer for the value 0x60000000. Packets punt to RP can also be sniffed by specifying a particular location using the command `show controllers events punt-sniff word1 0x60000000 34`.

**Examples**

Because you are executing this command on the line card, you must use the `execute-on` command to use the `show` command, or you must connect to the card using the `attach` command. All examples in this section use the `execute-on` command

The following is partial sample output from the `show controllers atm` command:

```
Router# execute-on slot 4 show controllers atm 0
TX SAR (Beta 1.0.0) is Operational;
RX SAR (Beta 1.0.0) is Operational;

Interface Configuration Mode:
STS-12c

Active Maker Channels: total # 6
VCID ChnnlID Type OutputInfo InPkts InOAMs MacString
 1 0888 UBR 0C010010 0 0 08882000AAAA030000000800
 2 0988 VBR 04010020 0 0 09882000
 3 8BC8 UBR 0C010030 0 0 8BC82000AAAA030000000800
 4 0E08 UBR 0C010040 0 0 0E082000AAAA030000000800
10 1288 VBR 040100A0 0 0 12882000
11 8BE8 VBR 0C0100B0 0 0 8BE82000AAAA030000000800

SAR Total Counters:
total_tx_idle_cells 215267 total_tx_paks 0 total_tx_abort_paks 0
total_rx_paks 0 total_rx_drop_paks 0 total_rx_discard_cells 15

Switching Code Counters:
total_rx_crc_err_paks 0 total_rx_giant_paks 0
total_rx_abort_paks 0 total_rx_crc10_cells 0
total_rx_tmout_paks 0 total_rx_unknown_paks 0

BATMAN Asic Register Values:
hi_addr_reg 0x8000, lo_addr_reg 0x0000, boot_mask_addr 0x0780,
rmcell_mask_addr 0x0724, rmcnt_mask_addr 0x07C2, txbuf_mask_addr 0x070C,
...

CM622 SAR Boot Configuration:
txind_q_addr 0x14000 txcmd_q_addr 0x20000
...

SUNI-622 Framer Register Values:
Master Rst and Ident/Load Meters Reg (#0x0): 0x10
Master Configuration Reg (#0x1): 0x1F
Master Interrupt Status Reg (#0x2): 0x00
PISO Interrupt Reg (#0x3): 0x04
Master Auto Alarm Reg (#0x4): 0x03
Master Auto Alarm Reg (#0x5): 0x07
Parallel Output Port Reg (#0x6): 0x02
```
The following is partial sample output from the `show controllers` command:

```
Router# execute-on slot 6 show controllers
Interface POS0
Hardware is BFLC POS
lcppos_instance struct 60311B40
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000400
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop
Interface POS1
Hardware is BFLC POS
lcppos_instance struct 603142E0
RX POS ASIC addr space 12000000
TX POS ASIC addr space 12000100
SUNI framer addr space 12000600
SUNI rsop intr status 00
CRC32 enabled, HDLC enc, int clock
no loop
```

The following is partial sample output from the `show controllers pos framers` command:

```
Router# execute-on slot 6 show controllers pos framers
Framer 0, addr=0x12000400:
master reset C0
master config 1F rrate sts3c trate sts3c fixptr
master control 00
clock rcv ctrl D0
RACP control 84
RACP gfc control 0F
TACP control status 04 hcsadd
RACP intr enable 04
RSOP ctrl intr enable 00
RSOP intr status 00
TPOP path sig lbl (c2) 13
SPTB control 04 tnull
SPTB status 00
Framer 1, addr=0x12000600:
master reset C0
master config 1F rrate sts3c trate sts3c fixptr
master control 00
clock rcv ctrl D0
RACP control 84
RACP gfc control 0F
TACP control status 04 hcsadd
RACP intr enable 04
RSOP ctrl intr enable 00
RSOP intr status 00
TPOP path sig lbl (c2) 13
SPTB control 04 tnull
```
The following is partial sample output from the `show controllers fia` command:

```
Router# execute-on slot 7 show controllers fia
========= Line Card (Slot 7) =======
Fabric configuration: Full bandwidth redundant
Master Scheduler: Slot 17
From Fabric FIA Errors
-----------------------
redund fifo parity 0       redund overflow 0       cell drops 0
 crc32 lkup parity 0       cell parity 0           crc32 0
0          1          2          3          4
-----------------------
los 0          0          0          0          0
crc16 0         0          0          0          0
To Fabric FIA Errors
-----------------------
sca not pres 0       req error 0       uni fifo overflow 0
grant parity 0       multi req 0       uni fifo undrflow 0
cntrl parity 0       uni req 0         crc32lkuparity 0
multi fifo 0         empty dst req 0  handshake error 0
```

The following is a sample output from the `show controllers events` command:

```
Router# execute-on slot 7 show controllers events
Switching Stats
   Packets punt to RP: 935
   HW engine punt: 62
   HW engine reject: 38113520
RX HW Engine Reject Counters
   Unrecognized Protocol ID: 19182546
   IP TTL Expired: 14706652
   Unrecognized L2 Frame: 4224320
   IPv6 Control pkts: 2
```

The following is a sample output from the `show controllers events punt-verbose` command:

```
Router# execute-on slot 7 show controllers events punt-verbose
RP Punted L2 Statistics in Verbose
------------------------------------
HDLC Encap : 927
RP Punted L3 Statistics in Verbose
------------------------------------
ICMP : 40
```

Cisco IOS Configuration Fundamentals Command Reference
The following is a partial sample output from the `show controllers events punt-verbose` all command which displays the zero and non-zero value of packets punt to RP from LC:

```
Router# execute-on slot 7 show controllers events punt-verbose all
RP Punted L2 Statistics in Verbose
------------------------------------
L2 Protocol - 0 : 0
ARPA Encap : 0
L2 Protocol - 2 : 0
L2 Protocol - 3 : 0
L2 Protocol - 4 : 0
HDLC Encap : 941
L2 Protocol - 6 : 0
L2 Protocol - 7 : 0
L2 Protocol - 8 : 0
L2 Protocol - 9 : 0
L2 Protocol - 10 : 0
L2 Protocol - 11 : 0
L2 Protocol - 12 : 0
L2 Protocol - 13 : 0
L2 Protocol - 14 : 0
L2 Protocol - 15 : 0
PPP Encap : 0
L2 Protocol - 17 : 0
L2 Protocol - 18 : 0
L2 Protocol - 19 : 0
Frame Relay Encap : 0
L2 Protocol - 21 : 0
L2 Protocol - 22 : 0
L2 Protocol - 23 : 0
L2 Protocol - 24 : 0
L2 Protocol - 25 : 0
L2 Protocol - 26 : 0
L2 Protocol - 27 : 0
L2 Protocol - 28 : 0
L2 Protocol - 29 : 0
L2 Protocol - 30 : 0
L2 Protocol - 31 : 0
L2 Protocol - 32 : 0
ATM Encap : 0
L2 Protocol - 34 : 0
L2 Protocol - 35 : 0
RP Punted L3 Statistics in Verbose
------------------------------------
HOPOPT : 0
ICMP : 40
IGMP : 0
L3 Protocol - 3 : 0
IPINIP : 0
L3 Protocol - 5 : 0
RP Punted L3 Application Statistics in Verbose
-----------------------------------------------
MPLS OAM : 0
FTP : 0
FTPD : 0
```
The following is a sample output from the `show controllers events clear` command:

Router# execute-on slot 7 show controllers events clear
Drop, switching and reject counters cleared

The following is a sample output from the `show controllers events punt-sniff` command:

Router# execute-on slot 7 show controllers events punt-sniff
Punt Sniff Statistics
--------------------------------
Word Location Occurance
0x60000000 34 0
0xB6010102 37 5
Note: Location offset taken from the beginning of BufferHeader (32 bytes).

The following is a sample output from the `show controllers events punt-sniff word1 0x60000000` command. This command is used to sniff a packet with a hexa-decimal value 0x60000000 from the start of the buffer header of the packet being punt to RP:

Router# execute-on slot 7 show controllers events punt-sniff word1 0x60000000

The following is a sample output from the `show controllers events punt-sniff word1 0x60000000 34` command. This command is used to sniff a packet with a hexa-decimal value 0x60000000 at the location 34 from the start of the buffer header of the packet being punt to RP:

Router# execute-on slot 7 show controllers events punt-sniff word1 0x60000000 34

The following is a sample output from the `show controllers events punt-sniff none` command. This command is used to clear the counter of packets to be sniffed:

Router# execute-on slot 7 show controllers events punt-sniff none

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controllers</td>
<td>Resets the T1 or E1 controller.</td>
<td></td>
</tr>
</tbody>
</table>

### show controllers logging

To display logging information about a Versatile Interface Processor (VIP) card, use the `show controllers logging` command in privileged EXEC mode.

```
show controllers vip slot-number logging
```

**Syntax Description**
- `vip slot-number`: VIP slot number.

**Command Modes**
- Privileged EXEC
show controllers logging

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and whether console logging is enabled.

When enabled, “trap logging” allows messages to be sent to a remote host (a syslog server).

Examples

The following is sample output from the `show controllers logging` command:

```plaintext
Router# show controllers vip 1 logging
show logging from Slot 1:
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns)
  Console logging: disabled
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 24 messages logged
  Trap logging: level informational, 266 messages logged.
  Logging to 209.165.202.129
  Exception Logging size: 4096 bytes
  Count and timestamp logging messages: disabled
Log Buffer (8192 bytes):
  smallest_local_pool_entries = 256, global particles = 5149
  highest_local_visible_bandwidth = 155000
  00:00:05:%SYS-5-RESTART: System restarted --
  .
  .
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog logging</td>
<td>Shows general state of system logging (enabled or disabled), and status of logged messages (number of messages dropped, rate-limited, or flushed).</td>
</tr>
<tr>
<td>Console logging</td>
<td>Logging to the console port. Shows &quot;disabled&quot; or, if enabled, the severity level limit and number of messages logged. Enabled using the <code>logging console</code> command.</td>
</tr>
<tr>
<td>Monitor logging</td>
<td>Logging to the monitor (all TTY lines). Shows &quot;disabled&quot; or, if enabled, the severity level limit and number of messages logged. Enabled using the <code>logging monitor</code> command.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Buffer logging | Logging to the standard syslog buffer. Shows "disabled" or, if enabled, the severity level limit and number of messages logged.
| Enabled using the **logging buffered** command.

| Trap logging | Logging to a remote host (syslog host). Shows "disabled" or, if enabled, the severity level limit and number of messages logged.
| (The word "trap" means a trigger in the system software for sending error messages to a remote host.)
| Enabled using the **logging host** command. The severity level limit is set using the **logging trap** command.

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show logging</strong></td>
<td>Displays the state of logging (syslog).</td>
</tr>
</tbody>
</table>

---

**show controllers tech-support**

To display general information about a Versatile Interface Processor (VIP) card when reporting a problem, use the **show controllers tech-support** command in privileged EXEC mode.

```
show controllers vip slot-number tech-support
```

**Syntax Description**

| vip slot-number | VIP slot number. |

---

**Command Modes**

Privileged EXEC

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use this command to help collect general information about a VIP card when you are reporting a problem. This command displays the equivalent of the following **show** commands for the VIP card:

- `more system:running-config`
- `show buffers`
- `show controllers`
- `show interfaces`
- `show processes cpu`
- `show processes memory`
• show stacks
• show version

For a sample display of the **show controllers tech-support** command output, refer to these **show** commands.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>more system:running-config</td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td></td>
<td>show buffers</td>
<td>Displays statistics for the buffer pools on the network server.</td>
</tr>
<tr>
<td></td>
<td>show controllers</td>
<td>Displays information that is specific to the hardware.</td>
</tr>
<tr>
<td></td>
<td>show interfaces</td>
<td>Uses the <strong>show interfaces</strong> EXEC command to display ALC information.</td>
</tr>
<tr>
<td></td>
<td>show processes</td>
<td>Displays information about the active processes.</td>
</tr>
<tr>
<td></td>
<td>show processes memory</td>
<td>Displays memory used.</td>
</tr>
<tr>
<td></td>
<td>show stacks</td>
<td>Monitors the stack usage of processes and interrupt routines.</td>
</tr>
<tr>
<td></td>
<td>show tech-support</td>
<td>Displays general information about the router when reporting a problem.</td>
</tr>
<tr>
<td></td>
<td>show version</td>
<td>Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.</td>
</tr>
</tbody>
</table>

**show coverage history**

To display the system history table, use the **show coverage history** command in privileged EXEC mode.

```
show coverage history [ [all|first number-of-entries|last number-of-entries|status] ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional)</td>
<td>Displays the entire history table.</td>
</tr>
<tr>
<td>first</td>
<td>(Optional)</td>
<td>Displays the oldest entries in the history table.</td>
</tr>
<tr>
<td>number-of-entries</td>
<td>(Optional)</td>
<td>Number of entries to be displayed. The range is from 1 to 100000.</td>
</tr>
<tr>
<td>last</td>
<td>(Optional)</td>
<td>Displays the latest entries in the history table.</td>
</tr>
<tr>
<td>status</td>
<td>(Optional)</td>
<td>Displays the status of the history system.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **show coverage history** command. The output is self-explanatory.
Router# show coverage history status

History table size is 23 entries. 0 entries have been used.
Low-level count handler has been called 0 times.
There were 0 entries not traced due to recursion detection.
There were 0 entries not traced due to internal pauses.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coverage</td>
<td>Enables the system to record the history of the events.</td>
</tr>
</tbody>
</table>

**show data-corruption**

To display data inconsistency errors of the present software version, use the **show data-corruption** command in user EXEC or privileged EXEC mode.

**show data-corruption**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(22)SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS 2.3 XE</td>
<td>This command was integrated into Cisco IOS XE Release 2.3.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display all data inconsistency errors or the corrupt data. If there are no data errors, the “No data inconsistency errors have been recorded” message is displayed.

**Examples**

The following is sample output from **show data-corruption** command. The fields are self-explanatory.

Router# show data-corruption
Data inconsistency records for:
3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(24)T, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Compiled Thu 17-Dec-09 09:02 by xyz

Count Traceback
1842 60523c58, 616e85fc 60523c58 62a9f648
1: Jun 12 18:24:33.960
2: Jun 12 18:24:33.960
show debugging

To display information about the types of debugging that are enabled for your router, use the show debugging command in privileged EXEC mode.

**show debugging**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>The output of this command was enhanced to show TCP Explicit Congestion Notification (ECN) configuration.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The output of this command was enhanced to show the user-group debugging configuration.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the show debugging command. In this example, the remote host is not configured or connected.

```
Router# show debugging
!
TCP:
  TCP Packet debugging is on
  TCP ECN debugging is on
!
Router# telnet 10.1.25.234
!
Trying 10.1.25.234 ...
!
00:02:48: 10.1.25.31:11001 <---> 10.1.25.234:23 out ECN-setup SYN
00:02:48: tcp0: O CLOSED 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
  OPTS 4 ECE CWR SYN WIN 4128
00:02:50: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:50: cwnd from 1460 to 1460, ssthresh from 65535 to 2920
00:02:54: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
  OPTS 4 ECE CWR SYN WIN 4128
00:02:54: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:54: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:02:54: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
  OPTS 4 ECE CWR SYN WIN 4128
```
The following is sample output from the show debugging command when user-group debugging is configured:

Router# show debugging
!
usergroup:
Usergroup Deletions debugging is on
Usergroup Additions debugging is on
Usergroup Database debugging is on
Usergroup API debugging is on
!

The following is sample output from the show debugging command when SNAP debugging is configured:

Router# show debugging

Persistent variable debugging is currently All
SNAP Server Debugging ON
SNAP Client Debugging ON

Router#

The table below describes the significant fields in the output.

Table 61: show debugging Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTS 4</td>
<td>Bytes of TCP expressed as a number. In this case, the bytes are 4.</td>
</tr>
<tr>
<td>ECE</td>
<td>Echo congestion experience.</td>
</tr>
<tr>
<td>CWR</td>
<td>Congestion window reduced.</td>
</tr>
</tbody>
</table>
### show declassify

To display the state of the declassify function (enabled, in progress, and so forth) and the sequence of declassification steps that will be performed, use the `show declassify` command in global configuration mode.

**show declassify**

**Syntax Description**

This command has no arguments or keywords.

**Note**

The `show declassify` command is supported on the Cisco 3200 series routers only.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)YD</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(2)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(2)T.</td>
</tr>
</tbody>
</table>

**Examples**

The following example is sample output for the `show declassify` command:

```
Router# show declassify
Declassify facility: Enabled=Yes  In Progress=No
   Erase flash=Yes  Erase nvram=Yes
   Obtain memory size
   Shutdown Interfaces
   Declassify Console and Aux Ports
   Erase flash
   Declassify NVRAM
   Declassify Communications Processor Module
   Declassify RAM, D-Cache, and I-Cache
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td>Synchronize connections--Request to synchronize sequence numbers, used when a TCP connection is being opened.</td>
</tr>
<tr>
<td>WIN 4128</td>
<td>Advertised window size, in bytes. In this case, the bytes are 4128.</td>
</tr>
<tr>
<td>cwnd</td>
<td>Congestion window (cwnd)--Indicates that the window size has changed.</td>
</tr>
<tr>
<td>ssthresh</td>
<td>Slow-start threshold (ssthresh)--Variable used by TCP to determine whether or not to use slow-start or congestion avoidance.</td>
</tr>
<tr>
<td>usergroup</td>
<td>Statically defined usergroup to which source IP addresses are associated.</td>
</tr>
</tbody>
</table>
Table 62: show declassify Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>A “Yes” value indicates that zeroization is enabled. A “No” value indicates that zeroization is disabled.</td>
</tr>
<tr>
<td>In Progress</td>
<td>A “Yes” value indicates that zeroization is currently in progress. A “No” value indicates that zeroization is currently not in progress.</td>
</tr>
<tr>
<td>Erase flash</td>
<td>A “Yes” value indicates that erasure of Flash memory is enabled. A “No” value indicates that the erasure of Flash memory is disabled.</td>
</tr>
<tr>
<td>Erase nvram</td>
<td>A “Yes” value indicates that the erasure of NVRAM is enabled. A “No” value indicates that the erasure of NVRAM is disabled.</td>
</tr>
<tr>
<td>Obtain memory size</td>
<td>Obtain the main memory size in order to understand how much of the memory is to be scrubbed.</td>
</tr>
<tr>
<td>Shutdown Interfaces</td>
<td>Shut down any and all network interfaces.</td>
</tr>
<tr>
<td>Declassify Console and AUX Ports</td>
<td>Remove potentially sensitive information from console and AUX port FIFOs.</td>
</tr>
<tr>
<td>Erase flash</td>
<td>Erase Flash memory.</td>
</tr>
<tr>
<td>Declassify NVRAM</td>
<td>Erase NVRAM.</td>
</tr>
<tr>
<td>Declassify Communications Processor Module</td>
<td>Erase the memory in the Communications Processor Module (CPM).</td>
</tr>
<tr>
<td>Declassify RAM, D-Cache, and I-Cache</td>
<td>Scrub the main memory, erase the Data Cache (D-Cache), and erase the Instruction Cache (I-Cache).</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service declassify</td>
<td>Invokes declassification.</td>
</tr>
</tbody>
</table>

show derived-config

To display the composite results of all the configuration commands that apply to an interface, including commands that come from sources such as static templates, dynamic templates, dialer interfaces, and authentication, authorization, and accounting (AAA) per-user attributes, use the **show derived-config** command in privileged EXEC mode.

**show derived-config [interface type number]**
**Syntax Description**

Optional) Displays the derived configuration for a specific interface. If you use the `interface` keyword, you must specify the interface type and the interface number (for example, `interface ethernet 0`).

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.1(2)S</td>
<td>This command was modified. The output was extended to include information about service instances and xconnects that are downloaded and provisioned.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configuration commands can be applied to an interface from sources such as static templates, dynamic templates bound by resource pooling, dialer interfaces, AAA per-user attributes and the configuration of the physical interface. The `show derived-config` command displays all the commands that apply to an interface.

The output for the `show derived-config` command is nearly identical to that of the `show running-config` command. It differs when the configuration for an interface is derived from a template, a dialer interface, or some per-user configuration. In those cases, the commands derived from the template, dialer interface, and so on, will be displayed for the affected interface.

If the same command is configured differently in two different sources that apply to the same interface, the command coming from the source that has the highest precedence will appear in the display.

On Performance Routing Version 3 (PfRv3) configured device, this command is used to display automatically configured components.

**Examples**

The following examples show sample output for the `show running-config` and `show derived-config` commands for serial interface 0:23 and dialer interface 0. The output of the `show running-config` and `show derived-config` commands is the same for dialer interface 0 because none of the commands that apply to that interface are derived from any sources other than the configuration of the dialer interface. The output for the `show running-config` and `show derived-config` commands for serial interface 0:23 differs because some of the commands that apply to serial interface 0:23 come from dialer interface 0.

```
Router# show running-config interface Serial0:23
Building configuration...
Current configuration :296 bytes
!
interface Serial0:23
   description PRI to ADTRAN (#4444150)
   ip unnumbered Loopback0
   encapsulation ppp
dialer rotary-group 0
   isdn switch-type primary-dms100
   isdn incoming-voice modem
   isdn calling-number 4444150
   peer default ip address pool old_pool
end

Router# show running-config interface Dialer0
Building configuration...
Current configuration :257 bytes
```
! interface Dialer0
description Dialin Users
ip unnumbered Loopback0
no ip proxy-arp
encapsulation ppp
dialer in-band
dialer idle-timeout 30
dialer-group 1
peer default ip address pool new_pool
ppp authentication pap chap callin
end
Router# show derived-config interface Serial0:23
Building configuration...
Derived configuration :332 bytes
!
interface Serial0:23
description PRI to ADTRAN (#4444150)
ip unnumbered Loopback0
encapsulation ppp
dialer roatry-group 0
isdn switch-type primary-dms100
isdn incoming-voice modem
isdn calling-number 4444150
peer default ip address pool new_pool
ppp authentication pap chap callin
end
Router# show derived-config interface Dialer0
Building configuration...
Derived configuration :257 bytes
!
interface Dialer0
description Dialin Users
ip unnumbered Loopback0
no ip proxy-arp
encapsulation ppp
dialer in-band
dialer idle-timeout 30
dialer-group 1
peer default ip address pool new_pool
ppp authentication pap chap callin
end

The following sample output from the show running-config and show derived-config commands show service instance and xconnect configurations.

Router# show running-config interface ethernet 0/0
Building configuration...

Current configuration : 201 bytes
!
interface Ethernet0/0
no ip address
service-policy type control mypolicy
service instance dynamic 1 ethernet
encapsulation dot1q 2-99
ethernet subscriber
initiator unclassified vlan
!
end

Router# show derived-config interface ethernet 0/0

Cisco IOS Configuration Fundamentals Command Reference
Building configuration...

Derived configuration: 306 bytes

! interface Ethernet0/0
  no ip address
  service-policy type control mypolicy
  service instance dynamic 1 ethernet
  encapsulation dot1q 2-99
  ethernet subscriber
  initiator unclassified vlan
  !
  service instance 2 ethernet
  encapsulation dot1q 22
  xconnect 33.33.33.34 12346 encapsulation mpls
  !
end

This following is a sample output of the `show derived-config | section eigrp` command displaying that EIGRP SAF is automatically configured.

Check the following fields in the output to ensure that the hub-master controller is configured accurately:

- EIGRP SAF configuration is auto-enabled
- EIGRP SAF peering status between hub and branch sites

HubMC# show derived-config | section eigrp

```
router eigrp #AUTOCFG# (API-generated auto-configuration, not user configurable)
  !
  service-family ipv4 autonomous-system 59501
  !
  sf-interface Loopback0
  hello-interval 120
  hold-time 600
  exit-sf-interface
  !
  topology base
  exit-sf-topology
  remote-neighbors source Loopback0 unicast-listen
  exit-service-family
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific interface.</td>
</tr>
</tbody>
</table>

**show diagnostic cns**

To display the information about the CNS subject, use the `show diagnostic cns` command in user EXEC or privileged EXEC mode.

```
show diagnostic cns {publish|subscribe}
```
Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publish</td>
<td>Displays the subject with which the diagnostic results is published.</td>
</tr>
<tr>
<td>subscribe</td>
<td>Displays the subscribed subjects.</td>
</tr>
</tbody>
</table>

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The CNS subsystem communicates with remote network applications through the CNS-event agent and follows the publish and subscribe model. An application sets itself up to receive events by subscribing to the appropriate event subject name.

Examples

This example shows how to display the subject with which the diagnostic results is published:

Router# show diagnostic cns publish

Subject: cisco.cns.device.diag_results

This example shows how to display the subscribed subject:

Router# show diagnostic cns subscribe

Subject: cisco.cns.device.diag_get_results

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic cns</td>
<td>Configures the CNS diagnostics.</td>
</tr>
</tbody>
</table>

show diagnostic sanity

To display sanity check results, use the show diagnostic sanity command in privileged EXEC mode.

Syntax Description

This command has no arguments or keywords.

Command Default

Displays information for all the Gigabit Ethernet WAN interfaces in the Cisco 7600 series router.

Command Modes

Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXE</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The sanity check runs a set of predetermined checks on the configuration with a possible combination of certain system states to compile a list of warning conditions. The checks are designed to look for anything that seems out of place and are intended to serve as an aid to maintaining the system sanity.

The following is a list of the checks that are run and the action taken when the condition is found:

- Checks whether the default gateways are reachable. If so, the system stops pinging.
- If a port auto-negotiates to half duplex, the system flags it.

Trunking Checks

- If a trunk port has the mode set to “on,” the system flags it.
- If a port is trunking and mode is auto, the system flags it.
- If a trunk port is not trunking and the mode is desirable, the system flags it.
- If a trunk port negotiates to half duplex, the system flags it.

Channeling Checks

- If a port has channeling mode set to on, the system flags it.
- If a port is not channeling and the mode is set to desirable, the system flags it.
- If a VLAN has a Spanning-Tree root of 32K (root is not set), the system flags it.

Spanning-Tree VLAN Checks

- If a VLAN has a max age on the Spanning-Tree root that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the Spanning-Tree root that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the bridge that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the bridge that is different than the default, the system flags it.
- If a VLAN has a hello time on the bridge that is different than the default, the system flags it.

Spanning-Tree Port Checks

- If a port has a port cost that is different than the default, the system flags it.
- If a port has a port priority that is different than the default, the system flags it.

UDLD Checks

- If a port has UDLD disabled, the system flags it.
- If a port had UDLD shut down, the system flags it.
• If a port had a UDLD undetermined state, the system flags it.

Assorted Port Checks
• If a port had receive flow control disabled, the system flags it.
• If a trunk port had PortFast enabled, the system flags it.
• If an inline power port has any of the following states:
  • denied
  • faulty
  • other
  • off

The system flags it.
• If a port has a native VLAN mismatch, the system flags it.
• If a port has a duplex mismatch, the system flags it.

Bootstrap and Config Register Checks
• The config register on the primary supervisor engine (and on the secondary supervisor engine if present) must be one of the following values: 0x2, 0x102, or 0x2102.
• The system verifies the bootstring on the primary supervisor engine (and on the secondary supervisor engine if present). The system displays a message if the bootstring is empty.
• The system verifies that every file is specified in the bootstring. The system displays a message if the file is absent or shows up with a wrong checksum.

If only device is specified as a filename, then the system verifies that the first file is on the device.

Assorted Checks
• The system displays a message if IGMP snooping is disabled.
• The system displays a message if any of the values of the snmp community access strings {RO,RW,RW-ALL} is the same as the default.
• The system displays a message if any of the modules are in states other than “Ok.”
• The system displays a message that lists all the tests that failed (displayed as an “F”) in the show test all command.
• The system displays a message if *fast is not configured on the switch anywhere.
• The system displays a message if there is enough room for the crashinfo file on the bootflash:.
• The system displays a message if multicast routing is enabled globally but is not applied to all interfaces.
• The system displays a message if IGMP snooping is disabled and RGMP is enabled.

Examples
This example displays samples of the messages that could be displayed with the show diagnostic sanity command:
Router# show diagnostic sanity
Pinging default gateway 10.6.141.1 ....
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.141.1, timeout is 2 seconds:
..!!.
Success rate is 0 percent (0/5)
IGMP snooping disabled please enable it for optimum config.
IGMP snooping disabled but RGMP enabled on the following interfaces,
please enable IGMP for proper config :
Vlan1, Vlan2, GigabitEthernet1/1
Multicast routing is enabled globally but not enabled on the following interfaces:
GigabitEthernet1/1, GigabitEthernet1/2
A programming algorithm mismatch was found on the device bootflash:
Formatting the device is recommended.
The bootflash: does not have enough free space to accomodate the crashinfo file.
Please check your confreg value : 0x0.
Please check your confreg value on standby: 0x0.
The boot string is empty. Please enter a valid boot string .
Could not verify boot image "disk0:" specified in the boot string on the slave.
Invalid boot image "bootflash:asdasd" specified in the boot string on the slave.
Please check your boot string on the slave.
UDLD has been disabled globally - port-level UDLD sanity checks are being bypassed.
OR
[ The following ports have UDLD disabled. Please enable UDLD for optimum config:
Fa9/45
The following ports have an unknown UDLD link state. Please enable UDLD on both sides of the link:
Fa9/45
]
The following ports have portfast enabled:
Fa9/35, Fa9/45
The following ports have trunk mode set to on:
Fa4/1, Fa4/13
The following trunks have mode set to auto:
Fa4/2, Fa4/3
The following ports with mode set to desirable are not trunking:
Fa4/3, Fa4/4
The following trunk ports have negotiated to half-duplex:
Fa4/3, Fa4/4
The following ports are configured for channel mode on:
Fa4/1, Fa4/2, Fa4/3, Fa4/4
The following ports, not channeling are configured for channel mode desirable:
Fa4/14
The following vlan(s) have a spanning tree root of 32768:
1
The following vlan(s) have max age on the spanning tree root different from the default:
1-2
The following vlan(s) have forward delay on the spanning tree root different from the default:
1-2
The following vlan(s) have hello time on the spanning tree root different from the default:
1-2
The following vlan(s) have max age on the bridge different from the default:
The following VLAN(s) have fwd delay on the bridge different from the default:
1-2
The following VLAN(s) have hello time on the bridge different from the default:
1-2
The following VLAN(s) have a different port priority than the default on the port FastEthernet4/1
1-2
The following ports have receive flow control disabled:
Fa9/35, Fa9/45
The following inline power ports have power-deny/faulty status:
Gi7/1, Gi7/2
The following ports have negotiated to half-duplex:
Fa9/45
The following VLANs have a duplex mismatch:
Fast 9/45
The following interfaces have a native VLAN mismatch:
interface (native VLAN - neighbor VLAN)
Fast 9/45 (1 - 64)
The value for Community-Access on read-only operations for SNMP is the same as default. Please verify that this is the best value from a security point of view.
The value for Community-Access on write-only operations for SNMP is the same as default. Please verify that this is the best value from a security point of view.
The value for Community-Access on read-write operations for SNMP is the same as default. Please verify that this is the best value from a security point of view.
Please check the status of the following modules:
8,9
Module 2 had a MINOR_ERROR.
The Module 2 failed the following tests:
TestIngressSpan
The following ports from Module2 failed test1:
1,2,4,48

**show disk**

To display flash or file system information for a disk, use the `show disk` command in user or privileged EXEC mode.

```
show {disk0|disk1} [{all|filesys}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>disk0</th>
<th>disk1</th>
<th>all</th>
<th>filesys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects disk 0 as the disk to display information about.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selects disk 1 as the disk to display information about.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional) Specifies that all flash information will be displayed for the selected disk.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional) Specifies that file system information will be displayed for the selected disk.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced in a release prior to Cisco IOS Release 12.2.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was enhanced to display information about the ATA ROM monitor library (monlib) file.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into the Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `show disk` command is supported only on platforms that have a disk file system.

Note

The name of the ATA monlib file may contain a platform name that does not match the platform that you are using. Different platforms may have a similar or the same name for their ATA monlib file.

Examples

The following example displays information about disk 0. The output is self-explanatory.

```
Router# show disk0 all
  -#- --length-- -----date/time------ path
1 19539160 Jan 27 2004 23:08:40 c7200-is-mz.123-5.7.P13a
1011679232 bytes available (19546112 bytes used)
******** ATA Flash Card Geometry/Format Info ********
ATA CARD GEOMETRY
Manufacturer Name            SMART ATA Flash Card
Model Number                SMART ATA FLASH DISK
Serial Number               00000155000000704162
Firmware Revision           V1.01
Number of Heads:            16
  Number of Cylinders       1999
  Sectors per Track        63
  Sector Size              512
  Total Sectors            2014992
ATA CARD FORMAT
  Number of FAT Sectors    246
  Sectors Per Cluster      32
  Number of Clusters       62941
  Number of Data Sectors   2014789
  Base Root Sector         632
  Base FAT Sector          140
  Base Data Sector         664
ATA MONLIB INFO
  Image Monlib size        67256
  Disk monlib size         71680
  Name                     c7200-atafslib-m
  Monlib Start sector      2
  Monlib End sector        133
  Monlib updated by        C7200-IS-ML2.3(5.7)P13a
  Monlib version           1
```
show disk0:

To display flash or file system information for a disk located in slot 0, use the `show disk0:` command in user EXEC or privileged EXEC mode.

`show disk0: [all|filesys]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) The <code>all</code> keyword displays complete information about flash memory, including information about the individual devices in flash memory and the names and sizes of all system image files stored in flash memory, including those that are invalid.</td>
</tr>
<tr>
<td>filesys</td>
<td>(Optional) Displays the device information block, the status information, and the usage information.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2</td>
<td>This command was incorporated into Cisco IOS Release 12.2.</td>
</tr>
<tr>
<td>12.3(T)</td>
<td>This command was enhanced to display information about the ATA ROM monitor library (monlib) file.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show disk0:` command is supported only on platforms that have a disk file system located in slot 0. Use the `show disk0:` command to display details about the files in a particular ATA PCMCIA flash disk memory card.

For more information regarding file systems and flash cards, access the `PCMCIA Filesystem Compatibility Matrix and Filesystem Information` document at the following URL:


**Note**

The name of the ATA monlib file may contain a platform name that does not match the platform that you are using. Different platforms may have a similar name or the same name for their ATA monlib file.

**Examples**

The following examples show displays of information about the flash disks or file system information for a disk. The output is self-explanatory.

```
c7200# show disk0:
  #-# --length-- -----date/time------ path
  1  29505176 Feb 27 2006 17:56:52 +00:00 c7200-jk9o3s-mz.124-6.T
  2  32768 Feb 24 2006 13:30:30 +00:00 file1.log
34738176 bytes available (29540352 bytes used)
c7200# show disk0: all
  #-# --length-- -----date/time------ path
```
This example shows how to update and display the time settings on a device using the `show disk0` command.
show disk1:

To display flash or file system information for a disk located in slot 1, use the show disk1: command in user EXEC or privileged EXEC mode.

```
show disk1:[{all/filesys}]
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dir disk0:</code></td>
<td>Displays a directory listing of files on an ATA PCMCIA flash disk card located in slot 0.</td>
</tr>
<tr>
<td><code>dir disk1:</code></td>
<td>Displays a directory listing of files on an ATA PCMCIA flash disk card located in slot 1.</td>
</tr>
<tr>
<td><code>show disk1:</code></td>
<td>Displays flash or file system information for a disk located in slot 1.</td>
</tr>
</tbody>
</table>

### Syntax Description

- **all** (Optional) The `all` keyword displays complete information about flash memory, including information about the individual devices in flash memory and the names and sizes of all system image files stored in flash memory, including those that are invalid.
- **filesys** (Optional) Displays the device information block, the status information, and the usage information.

### Command Modes

- User EXEC
- Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2</td>
<td>This command was incorporated into Cisco IOS Release 12.2.</td>
</tr>
</tbody>
</table>
Modification/Release

This command was enhanced to display information about the ATA ROM monitor library (monlib) file.

12.3(7)T

This command was integrated into Cisco IOS Release 12.2(25)S.

12.2(33)SRA

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

Usage Guidelines

The `show disk1:` command is supported only on platforms that have a disk file system. Use the `show disk01:` command to display details about the files in a particular ATA PCMCIA flash disk memory card located in slot 1.

For more information regarding file systems and flash cards, access the PCMCIA Filesystem Compatibility Matrix and Filesystem Information document at the following URL:


Note

The name of the ATA monlib file may contain a platform name that does not match the platform that you are using. Different platforms may have a similar name or the same name for their ATA monlib file.

Examples

The following examples show displays of information about the flash disks or file system information for a disk. The output is self-explanatory.

c7200# show disk1:
-#- --length-- -----date/time------ path
1 29505176 Feb 27 2006 17:56:52 +00:00 c7200-jk9o3s-mz.124-6.T
2 32768 Feb 24 2006 13:30:30 +00:00 file1.log
34738176 bytes available (29540352 bytes used)
c7200# show disk1: all
-#- --length-- -----date/time------ path
1 29505176 Feb 27 2006 17:56:52 +00:00 c7200-jk9o3s-mz.124-6.T
2 32768 Feb 24 2006 13:30:30 +00:00 file1.log
34738176 bytes available (29540352 bytes used)
******* ATA Flash Card Geometry/Format Info *******
ATA CARD GEOMETRY
   Number of Heads:  4
   Number of Cylinders  984
   Sectors per Cylinder  32
   Sector Size  512
   Total Sectors  125952
ATA CARD FORMAT
   Number of FAT Sectors  62
   Sectors Per Cluster  8
   Number of Clusters  15693
   Number of Data Sectors  125812
   Base Root Sector  232
   Base FAT Sector  108
   Base Data Sector  264
ATA MONLIB INFO
   Image Monlib size =  73048
   Disk monlib size =  55296
   Name = NA
   Monlib end sector = NA
   Monlib Start sector = NA
show environment

To display temperature, voltage, fan, and power supply information, use the `show environment` command in user EXEC or privileged EXEC mode.

```
show environment command
show environment command
[ { alarms | all | fans | hardware | last | leds | power-supply | table | temperature | voltages } ]
```

Cisco 7000 Series, Cisco 7200 Series, Cisco 7304, and Cisco 7500 Series

```
show environment command
[ { all | last | table } ]
```

Cisco ASR 1000 Series

```
show environment [ { all | counters | history | sensor | location | sensor | sensor | sensor | table | sensor } ]
```

Cisco uBR10012 Routers

```
show environment [ { all | last | subslot slot / subslot | table } ]
```

**Syntax Description**

<p>| alarms | (Optional) Displays the alarm contact information. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Displays a detailed listing of all environmental monitor parameters (for example, the power supplies, temperature readings, voltage readings, and blower speeds). This is the default.</td>
</tr>
<tr>
<td>fans</td>
<td>(Optional) Displays blower and fan information.</td>
</tr>
<tr>
<td>hardware</td>
<td>(Optional) Displays hardware-specific information.</td>
</tr>
<tr>
<td>last</td>
<td>(Optional) Displays information on the last measurement made.</td>
</tr>
<tr>
<td>leds</td>
<td>(Optional) Displays the status of the MBus LEDs on the clock and scheduler cards and switch fabric cards.</td>
</tr>
<tr>
<td>power-supply</td>
<td>(Optional) Displays power supply voltage and current information. If applicable, displays the status of the redundant power supply.</td>
</tr>
<tr>
<td>table</td>
<td>(Optional) Displays the temperature, voltage, and blower ranges and thresholds. On the Cisco 7200 series, including the NPE-G2 in the Cisco 7200 VXR, the Cisco 7304 routers, and the Cisco 7500 series routers, the table keyword displays only the temperature and voltage thresholds.</td>
</tr>
<tr>
<td>temperature</td>
<td>(Optional) Displays temperature information.</td>
</tr>
<tr>
<td>voltages</td>
<td>(Optional) Displays voltage information.</td>
</tr>
<tr>
<td>counters</td>
<td>Displays operational counters.</td>
</tr>
<tr>
<td>history</td>
<td>Displays sensor state change history.</td>
</tr>
<tr>
<td>location</td>
<td>Displays sensors by location.</td>
</tr>
<tr>
<td>sensor</td>
<td>Displays sensor summary.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays a summary of all the environment monitoring sensors</td>
</tr>
<tr>
<td>sensor</td>
<td>Sensor name.</td>
</tr>
<tr>
<td>subslot</td>
<td>(Optional) Displays environmental monitor parameters for a subslot.</td>
</tr>
<tr>
<td>slot</td>
<td>Slot number. Valid values range from 1 to 8.</td>
</tr>
<tr>
<td>subslot</td>
<td>Subslot number. Valid values are 0 and 1.</td>
</tr>
</tbody>
</table>

**Command Default**

If no options are specified, the default is `all`.

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The availability of keywords depends on your system and platform. The command does not support SPAs on the Cisco 7200 series and on the NPE-G2 in the Cisco 7200 VXR routers.

A routine runs once a minute that reads environmental measurements from sensors and stores the output into a buffer. For shared port adapters (SPAs), the temperature and voltage sensors are read every few seconds to get environmental data. The environmental buffer is displayed on the console when you use the `show environment` command.

If a measurement exceeds desired margins, but has not exceeded fatal margins, a warning message is printed to the system console. The system software queries the sensors for measurements once a minute, but warnings for a given test point are printed at most once every hour for sensor readings in the warning range and once every 5 minutes for sensor readings in the critical range. If a measurement is out of line within these time segments, an automatic warning message appears on the console. As noted, you can query the environmental status with the `show environment` command at any time to determine whether a measurement is at the warning or critical tolerance.

A SPA is shut down when any of the SPA environment readings exceed the shutdown threshold.

If a shutdown occurs because of detection of fatal environmental margins, the last measured value from each sensor is stored in internal nonvolatile memory.

For environmental specifications, refer to the hardware installation and configuration publication for your individual chassis.

For network processor engines (NPEs), network services engines (NSEs), line cards, and modular services cards (MSCs), environmental information is recorded in the CISCO-ENVMON-MIB. SPAs are not supported by the CISCO-ENVMON-MIB. In Cisco IOS Release 12.2(20)S2 and later, the CISCO-ENTITY-SENSOR-MIB supports environmental information for SPAs, as well as NPEs, NSEs, line cards, and MSCs.
If the Cisco 12000 series GSR exceeds environmental conditions, a message similar to the following is displayed on the console:

%GSR_ENV-2-WARNING: Slot 3 Hot Sensor Temperature exceeds 40 deg C;
Check cooling systems

Blower temperatures that exceed environmental conditions do not generate a warning message.

You can also enable Simple Network Management Protocol (SNMP) notifications (traps or informs) to alert a network management system (NMS) when environmental thresholds are reached using the `snmp-server enable traps envmon` and `snmp-server host` global configuration commands.

Whenever Cisco IOS software detects a failure or recovery event from the DRPS unit, it sends an SNMP trap to the configured SNMP server. Unlike console messages, only one SNMP trap is sent when the failure event is first detected. Another trap is sent when the recovery is detected.

Cisco AS5300 DRPS software reuses the MIB attributes and traps defined in CISCO-ENVMON-MIB and CISCO-ACCESS-ENVMON-MIB. CISCO-ENVMON-MIB is supported by all Cisco routers with RPS units, and CISCO-ACCESS-ENVMON-MIB is supported by the Cisco 3600 series routers.

A power supply trap defined in CISCO-ENVMON-MIB is sent when a failure is detected and when a failure recovery occurs for the following events: input voltage fail, DC output voltage fail, thermal fail, and multiple failure events.

A fan failure trap defined in CISCO-ENVMON-MIB is sent when a fan failure or recovery event is detected by Cisco IOS software.

A temperature trap defined in CISCO-ACCESS-ENVMON-MIB is sent when a board over-temperature condition is detected by Cisco IOS software.

CISCO-ACCESS-ENVMON-MIB also defines an over-voltage trap. A similar trap is defined in CISCO-ENVMON-MIB, but it requires the ciscoEnvMonVoltageStatusValue in varbinds. This value indicates the current value of the voltage in the RPS. With Cisco AS5300 RPS units, the current voltage value is not sent to the motherboard.

CISCO-ENVMON-MIB is extended to add a new enumerated value, internalRedundant(5), for MIB attribute ciscoEnvMonSupplySource. This is used to identify a RPS unit.

The temperature history of the Cisco uBR-MC20X20V line card, used in Cisco uBR10012 universal broadband router, can be viewed using the show environment subslot command. The show environment subslot command displays the thermal and power status of the Cisco uBR-MC20X20V line card. The slot/subslot option of the show environment subslot command helps to identify the location of the line card.

**Examples**

**Cisco ASR 1000 Series Routers**

In the following example, the show environment all command displays system temperature, voltage, fan, and power supply conditions. (It does not display environmental information for SPAs.) The State column in show environment all output should show “Normal” except for fans where it indicates fan speed. A fan speed of 65% is normal.

Router# show environment all
Sensor List:  Environmental Monitoring
<table>
<thead>
<tr>
<th>Sensor</th>
<th>Location</th>
<th>State</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1: VMA</td>
<td>F0</td>
<td>Normal</td>
<td>1801 mV</td>
</tr>
<tr>
<td>V1: VMB</td>
<td>F0</td>
<td>Normal</td>
<td>1206 mV</td>
</tr>
<tr>
<td>V1: VMC</td>
<td>F0</td>
<td>Normal</td>
<td>1206 mV</td>
</tr>
<tr>
<td>V1: VMD</td>
<td>F0</td>
<td>Normal</td>
<td>1103 mV</td>
</tr>
<tr>
<td>V1: VME</td>
<td>F0</td>
<td>Normal</td>
<td>1005 mV</td>
</tr>
<tr>
<td>V1: 12v</td>
<td>F0</td>
<td>Normal</td>
<td>11967 mV</td>
</tr>
<tr>
<td>V1: VDD</td>
<td>F0</td>
<td>Normal</td>
<td>3295 mV</td>
</tr>
<tr>
<td>V1: GP1</td>
<td>F0</td>
<td>Normal</td>
<td>905 mV</td>
</tr>
<tr>
<td>V2: VMA</td>
<td>F0</td>
<td>Normal</td>
<td>3295 mV</td>
</tr>
<tr>
<td>V2: VMB</td>
<td>F0</td>
<td>Normal</td>
<td>2495 mV</td>
</tr>
<tr>
<td>V2: VMC</td>
<td>F0</td>
<td>Normal</td>
<td>1499 mV</td>
</tr>
<tr>
<td>V2: VMD</td>
<td>F0</td>
<td>Normal</td>
<td>1098 mV</td>
</tr>
<tr>
<td>V2: VME</td>
<td>F0</td>
<td>Normal</td>
<td>1000 mV</td>
</tr>
<tr>
<td>V2: 12v</td>
<td>F0</td>
<td>Normal</td>
<td>11923 mV</td>
</tr>
<tr>
<td>V2: VDD</td>
<td>F0</td>
<td>Normal</td>
<td>3295 mV</td>
</tr>
<tr>
<td>V2: GP1</td>
<td>F0</td>
<td>Normal</td>
<td>751 mV</td>
</tr>
<tr>
<td>Temp: Inlet</td>
<td></td>
<td>Normal</td>
<td>27 Celsius</td>
</tr>
<tr>
<td>Temp: ASIC1</td>
<td></td>
<td>Normal</td>
<td>44 Celsius</td>
</tr>
<tr>
<td>Temp: Exhaust1</td>
<td></td>
<td>Normal</td>
<td>36 Celsius</td>
</tr>
<tr>
<td>Temp: Exhaust2</td>
<td></td>
<td>Normal</td>
<td>34 Celsius</td>
</tr>
<tr>
<td>Temp: ASIC2</td>
<td></td>
<td>Normal</td>
<td>40 Celsius</td>
</tr>
<tr>
<td>V1: VMA</td>
<td>0</td>
<td>Normal</td>
<td>1103 mV</td>
</tr>
<tr>
<td>V1: VMB</td>
<td>0</td>
<td>Normal</td>
<td>1201 mV</td>
</tr>
<tr>
<td>V1: VMC</td>
<td>0</td>
<td>Normal</td>
<td>1503 mV</td>
</tr>
<tr>
<td>V1: VMD</td>
<td>0</td>
<td>Normal</td>
<td>1801 mV</td>
</tr>
<tr>
<td>V1: VME</td>
<td>0</td>
<td>Normal</td>
<td>2495 mV</td>
</tr>
<tr>
<td>V1: VMF</td>
<td>0</td>
<td>Normal</td>
<td>3295 mV</td>
</tr>
<tr>
<td>V1: 12v</td>
<td>0</td>
<td>Normal</td>
<td>11967 mV</td>
</tr>
<tr>
<td>V1: VDD</td>
<td>0</td>
<td>Normal</td>
<td>3295 mV</td>
</tr>
<tr>
<td>V1: GP1</td>
<td>0</td>
<td>Normal</td>
<td>751 mV</td>
</tr>
<tr>
<td>V1: GP2</td>
<td>0</td>
<td>Normal</td>
<td>903 mV</td>
</tr>
<tr>
<td>V2: VMB</td>
<td>0</td>
<td>Normal</td>
<td>1201 mV</td>
</tr>
<tr>
<td>V2: 12v</td>
<td>0</td>
<td>Normal</td>
<td>11967 mV</td>
</tr>
<tr>
<td>V2: VDD</td>
<td>0</td>
<td>Normal</td>
<td>3291 mV</td>
</tr>
<tr>
<td>V2: GP2</td>
<td>0</td>
<td>Normal</td>
<td>903 mV</td>
</tr>
<tr>
<td>Temp: Left</td>
<td>0</td>
<td>Normal</td>
<td>28 Celsius</td>
</tr>
<tr>
<td>Temp: Center</td>
<td>0</td>
<td>Normal</td>
<td>30 Celsius</td>
</tr>
<tr>
<td>Temp: ASIC1</td>
<td>0</td>
<td>Normal</td>
<td>42 Celsius</td>
</tr>
<tr>
<td>Temp: Right</td>
<td>0</td>
<td>Normal</td>
<td>27 Celsius</td>
</tr>
<tr>
<td>V1: VMA</td>
<td>1</td>
<td>Normal</td>
<td>1103 mV</td>
</tr>
<tr>
<td>V1: VMB</td>
<td>1</td>
<td>Normal</td>
<td>1201 mV</td>
</tr>
<tr>
<td>V1: VMC</td>
<td>1</td>
<td>Normal</td>
<td>1503 mV</td>
</tr>
<tr>
<td>V1: VMD</td>
<td>1</td>
<td>Normal</td>
<td>1801 mV</td>
</tr>
<tr>
<td>V1: VME</td>
<td>1</td>
<td>Normal</td>
<td>2495 mV</td>
</tr>
<tr>
<td>V1: VMF</td>
<td>1</td>
<td>Normal</td>
<td>3295 mV</td>
</tr>
<tr>
<td>V1: 12v</td>
<td>1</td>
<td>Normal</td>
<td>11953 mV</td>
</tr>
<tr>
<td>V1: VDD</td>
<td>1</td>
<td>Normal</td>
<td>3291 mV</td>
</tr>
<tr>
<td>V1: GP1</td>
<td>1</td>
<td>Normal</td>
<td>754 mV</td>
</tr>
<tr>
<td>V1: GP2</td>
<td>1</td>
<td>Normal</td>
<td>903 mV</td>
</tr>
<tr>
<td>V2: VMB</td>
<td>1</td>
<td>Normal</td>
<td>1206 mV</td>
</tr>
<tr>
<td>V2: 12v</td>
<td>1</td>
<td>Normal</td>
<td>11967 mV</td>
</tr>
<tr>
<td>V2: VDD</td>
<td>1</td>
<td>Normal</td>
<td>3291 mV</td>
</tr>
<tr>
<td>V2: GP2</td>
<td>1</td>
<td>Normal</td>
<td>905 mV</td>
</tr>
<tr>
<td>Temp: Left</td>
<td>1</td>
<td>Normal</td>
<td>28 Celsius</td>
</tr>
<tr>
<td>Temp: Center</td>
<td>1</td>
<td>Normal</td>
<td>30 Celsius</td>
</tr>
<tr>
<td>Temp: ASIC1</td>
<td>1</td>
<td>Normal</td>
<td>44 Celsius</td>
</tr>
<tr>
<td>Temp: Right</td>
<td>1</td>
<td>Normal</td>
<td>28 Celsius</td>
</tr>
<tr>
<td>PEM Iout</td>
<td>P0</td>
<td>Normal</td>
<td>37 A</td>
</tr>
<tr>
<td>PEM Vout</td>
<td>P0</td>
<td>Normal</td>
<td>12 V AC</td>
</tr>
<tr>
<td>PEM Vin</td>
<td>P0</td>
<td>Normal</td>
<td>116 V AC</td>
</tr>
<tr>
<td>Temp: PEM</td>
<td>P0</td>
<td>Normal</td>
<td>28 Celsius</td>
</tr>
<tr>
<td>Temp: FC</td>
<td>P0</td>
<td>Fan Speed 65%</td>
<td>25 Celsius</td>
</tr>
</tbody>
</table>
The following table describes the significant fields shown in the display.

**Table 63: show environment all Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor</td>
<td>Sensor name.</td>
</tr>
<tr>
<td>Location</td>
<td>Chassis slot.</td>
</tr>
<tr>
<td>State</td>
<td>State description. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Critical--Critical alarm indicating a service-affecting condition.</td>
</tr>
<tr>
<td></td>
<td>• Fan Speed--Fan speed (65% is normal).</td>
</tr>
<tr>
<td></td>
<td>• Major--Major alarm indicating immediate action is needed.</td>
</tr>
<tr>
<td></td>
<td>• Minor--Minor alarm indicating warning conditions.</td>
</tr>
<tr>
<td></td>
<td>• Normal--Sensor reading is in acceptable range.</td>
</tr>
<tr>
<td></td>
<td>• Shutdown--If automatic shutdown is enabled, indicates that the router will shut down.</td>
</tr>
<tr>
<td>Reading</td>
<td>Voltage or temperature detected by the sensor.</td>
</tr>
</tbody>
</table>

**Cisco 7000 Series Routers, Cisco 7200 Series Routers**

In the following example, the typical `show environment` display is shown when no warning conditions are in the system for the Cisco 7000 series and Cisco 7200 series routers. This information may vary slightly depending on the platform you are using. The date and time of the query are displayed, along with the data refresh information and a message indicating that there are no warning conditions.

```router> show environment
Environmental Statistics
   Environmental status as of 13:17:39 UTC Thu Jun 6 1996
   Data is 7 second(s) old, refresh in 53 second(s)
   All Environmental Measurements are within specifications

The following table describes the significant fields shown in the display.
Table 64: show environment Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental status as of...</td>
<td>Current date and time.</td>
</tr>
<tr>
<td>Data is..., refresh in...</td>
<td>Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.</td>
</tr>
<tr>
<td>Status message</td>
<td>If environmental measurements are not within specification, warning messages are displayed.</td>
</tr>
</tbody>
</table>

NPE-G2 in Cisco 7200 VXR Routers

In the following example, additional temperature and voltage readings for the NPE-G2 in the Cisco 7200 VXR router are displayed by the show environment all command. Power supplies 1 and 2 are on, and all monitored variables are within the normal operating range.

```
Router_npe-g2# show environment all
Power Supplies:
Power Supply 1 is Zytek AC Power Supply. Unit is on.
Power Supply 2 is Zytek AC Power Supply. Unit is on.
Temperature readings:
NPE Inlet measured at 25C/77F
NPE Outlet measured at 28C/82F
CPU Die measured at 56C/132F
Voltage readings:
+3.30 V measured at +3.32 V
+1.50 V measured at +1.48 V
+2.50 V measured at +2.46 V
+1.80 V measured at +1.75 V
+1.20 V measured at +1.17 V
VDD_CPU measured at +1.28 V
VDD_MEM measured at +2.50 V
VTT measured at +1.25 V
+3.45 V measured at +3.39 V
-11.95 measured at -11.93 V
+5.15 V measured at +4.96 V
+12.15 V measured at +12.18 V
Envm stats saved 0 time(s) since reload
```

Table 65: show environment all Field Descriptions for NPE-G2 in Cisco 7200 VXR Router

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply x is present.</td>
<td>Specifies whether the indicated (x) power supply slot is populated. If a power supply slot is populated, the manufacturer name and whether it is an AC or DC power supply is displayed.</td>
</tr>
<tr>
<td>Unit is ...</td>
<td>Indicates whether the power supply status is on or off.</td>
</tr>
<tr>
<td>Temperature readings</td>
<td>Indicates the temperature of air coming in and going out of the NPE Inlet, NPE Outlet, and CPU Die areas.</td>
</tr>
</tbody>
</table>
Indicate that the temperature measurements at the inlet area of the chassis is 25C/77F, which is within normal operating range. System shutdown for NPE Inlet is 80C/176F.

Indicate that the temperature measurements at the outlet area of the chassis is 28C/82F, which is within normal operating range. System shutdown for NPE Outlet is 84C/183F.

Indicate that the temperature measurement at the CPU Die (internal silicon of the CPU) area of the chassis is 56C/132F, which is within normal operating range. System shutdown for CPU Die is 100C/212F.

System voltage measurements that indicate the actual measured value for the specified power rail, which is named after the expected target value. For example, the +3.30 V rail, with an expected value of +3.30 V, actually measures at +3.32 V. This is within the target range.

For example, the +1.50 V rail, with an expected value of +1.50 V, actually measures at +1.48 V. This is within the target range.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPE Inlet measured at 25C/77F</td>
<td>Indicates that the temperature measurements at the inlet area of the chassis is 25C/77F, which is within normal operating range. System shutdown for NPE Inlet is 80C/176F.</td>
</tr>
<tr>
<td>NPE Outlet measured at 28C/82F</td>
<td>Indicates that the temperature measurements at the outlet area of the chassis is 28C/82F, which is within normal operating range. System shutdown for NPE Outlet is 84C/183F.</td>
</tr>
<tr>
<td>CPU Die measured at 56C/132F</td>
<td>Indicates that the temperature measurement at the CPU Die (internal silicon of the CPU) area of the chassis is 56C/132F, which is within normal operating range. System shutdown for CPU Die is 100C/212F.</td>
</tr>
<tr>
<td>Voltage readings:</td>
<td>System voltage measurements that indicate the actual measured value for the specified power rail, which is named after the expected target value. For example, the +3.30 V rail, with an expected value of +3.30 V, actually measures at +3.32 V. This is within the target range. For example, the +1.50 V rail, with an expected value of +1.50 V, actually measures at +1.48 V. This is within the target range.</td>
</tr>
<tr>
<td>+3.30 V measured at +3.32 V</td>
<td></td>
</tr>
<tr>
<td>+1.50 V measured at +1.48 V</td>
<td></td>
</tr>
<tr>
<td>VDD_CPU measured at +1.28 V</td>
<td>Indicates +1.28 V is the measured voltage of the VDD_CPU power rail, which is within normal operating range. The expected value is 1.25 V.</td>
</tr>
<tr>
<td>VDD_MEM measured at +2.50 V</td>
<td>Indicates +2.50 V is the measured voltage of the VDD_MEM power rail, which is within normal operating range. The expected value is 2.5 V.</td>
</tr>
<tr>
<td>VTT measured at +1.25 V</td>
<td>Indicates +1.25 V is the measured voltage of the VTT power rail, which is within normal operating range. The expected value is 1.25 V.</td>
</tr>
</tbody>
</table>

In the following example, the show environment last command displays the previously saved measurements (readings) from the last environmental reading before the router was shut down. The command also displays the reason why the router was shut down, which was “power supply shutdown” in this case.

Router_npe-g2# show environment last
NPE Inlet previously measured at 26C/78F
NPE Outlet previously measured at 28C/82F
CPU Die previously measured at 56C/132F
+3.30 V previously measured at +3.32
+1.50 V previously measured at +1.48
+2.50 V previously measured at +2.46
+1.80 V previously measured at +1.75
+1.20 V previously measured at +1.17
VDD_CPU previously measured at +1.28
VDD_MEM previously measured at +2.50
VTT previously measured at +1.25
+3.45 V previously measured at +3.39
-11.95 previously measured at -11.93
+5.15 V previously measured at +4.96
+12.15 V previously measured at +12.18
last shutdown reason - power supply shutdown

Cisco IOS Configuration Fundamentals Command Reference
Table 66: show environment last Field Descriptions for NPE-G2 in Cisco 7200 VXR Router

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPE Inlet previously measured at 26C/78F</td>
<td>The last measured temperature of the inlet air of the router prior to shutdown.</td>
</tr>
<tr>
<td>NPE Outlet previously measured at 28C/82F</td>
<td>The last measured temperature of the outlet air of the router prior to shutdown.</td>
</tr>
<tr>
<td>CPU Die previously measured at 56C/132F</td>
<td>The last measured temperature of the CPU Die prior to shutdown.</td>
</tr>
<tr>
<td>+3.30 V previously measured at +3.32</td>
<td>The last measured voltage of the 3.30 V power rail prior to shutdown.</td>
</tr>
<tr>
<td>VDD_CPU previously measured at +1.28</td>
<td>The last measured voltage of the VDD_CPU power rail prior to shutdown.</td>
</tr>
<tr>
<td>VDD_MEM previously measured at +2.50</td>
<td>The last measured voltage of the VDD_MEM power rail prior to shutdown.</td>
</tr>
<tr>
<td>VTT previously measured at +1.25</td>
<td>The last measured voltage of the VTT power rail prior to shutdown.</td>
</tr>
<tr>
<td>last shutdown reason</td>
<td>Indicates the reason for the shutdown.</td>
</tr>
</tbody>
</table>

In the following example, the show environment table command displays threshold levels in a table format of the environmental monitor parameters. It displays the high warning, high critical, and high shutdown temperature thresholds of the NPE inlet, NPE outlet, and CPU Die. It also displays the low and high critical voltage thresholds, and low and high shutdown voltage thresholds for the power rails on the NPE-G2 in the Cisco 7200 VXR.

Note

The low range temperatures, such as the LowShut, LowCrit, and LowWarn temperature thresholds, are not checked and are not displayed on the NPE-G2. Also the warning voltage thresholds, such as LowWarn and HighWarn, are not checked and are not displayed on the NPE-G2.

Router_npe-g2# show environment table
Sample Point LowShut LowCrit LowWarn HighWarn HighCrit HighShut
NPE Inlet 44C/111F 59C/138F
NPE Outlet 49C/120F 64C/147F
CPU Die 75C/167F 85C/185F
System shutdown for NPE Inlet is 80C/176F
System shutdown for NPE Outlet is 84C/183F
System shutdown for CPU Die is 100C/212F
+3.30 V +2.30 +3.12 +3.47 +4.29
+1.50 V +1.05 +1.40 +1.56 +1.95
+2.50 V +1.71 +2.34 +2.61 +3.28
+1.80 V +1.25 +1.67 +1.91 +2.34
+1.20 V +0.82 +1.13 +1.28 +1.56
VDD_CPU +0.89 +1.21 +1.36 +1.71
VDD_MEM +1.71 +2.34 +2.61 +3.28
VTT +0.85 +1.17 +1.32 +1.64
+3.45 V +2.38 +3.28 +3.63 +4.49
Table 67: Field Descriptions for NPE-G2 in Cisco 7200 VXR Router

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Point</td>
<td>This is the area for which temperature or system voltage thresholds are displayed.</td>
</tr>
</tbody>
</table>
| LowShut | This is the LowShut voltage threshold. If the voltage value is below the LowShut threshold, the router shuts down.  
**Note** The LowShut temperature value is not checked and its threshold is not displayed on the NPE-G2. |
| LowCrit | This is the low critical voltage threshold. If the voltage value is below the LowCrit threshold, a critical message is issued for an out-of-tolerance voltage value. The system continues to operate. However, the system is approaching shutdown.  
**Note** The LowCrit temperature value is not checked and its threshold is not displayed on the NPE-G2. |
| LowWarn | The LowWarn temperature threshold and LowWarn voltage threshold are not checked and the threshold information is not displayed on the NPE-G2. |
| HighWarn | This is the HighWarn temperature threshold. If the temperature reaches the HighWarn threshold, a warning message is issued for an out-of-tolerance temperature value. The system continues to operate, but operator action is recommended to bring the system back to a normal state.  
**Note** The HighWarn voltage threshold is not checked and its threshold is not displayed on the NPE-G2. |
| HighCrit | This is the HighCrit temperature or voltage threshold. If the temperature or voltage reaches the HighCrit level, a critical message is issued. The system continues to operate. However, the system is approaching shutdown.  
**Note** Beware that if the temperature reaches or exceeds the HighShut value, a Shutdown message is issued and the router shuts down. |
| HighShut | This is the HighShut temperature or voltage threshold. If the temperature or voltage level reaches or exceeds the HighShut value, a Shutdown message is issued and the router shuts down. |
These are the HighWarn and HighCrit temperature thresholds, respectively, for the NPE Inlet.

If the NPE Inlet temperature value reaches the HighWarn (44°C/111°F) and HighCrit (59°C/138°F) levels, warning and critical messages, respectively, are issued.

If the value reaches 44°C/111°F or greater, you receive a warning message indicating HighWarn. The system continues to operate, but operator action is recommended to bring the system back to a normal state.

If the value reaches 59°C/138°F or greater, you receive a critical (HighCrit) message instead, that indicates the system continues to operate, but the system is approaching shutdown.

Note Beware if the temperature reaches or exceeds 80°C/176°F, which is the HighShut value, a Shutdown message is issued, and the NPE Inlet area shuts down.

These are the HighWarn and HighCrit temperature thresholds, respectively, for the NPE Outlet.

If the NPE Outlet temperature value reaches the HighWarn (49°C/120°F) and HighCrit (64°C/147°F) levels, warning and critical messages, respectively, are issued.

If the value reaches 49°C/120°F or greater, you receive a warning message indicating HighWarn. The system continues to operate, but operator action is recommended to bring the system back to a normal state.

If the value reaches 64°C/147°F or greater, you receive a critical (HighCrit) message instead that indicates the system continues to operate, but the system is approaching shutdown.

Note Beware if the temperature reaches or exceeds 84°C/183°F, which is the HighShut value, a Shutdown message is issued, and the NPE Outlet area shuts down.

These are the HighWarn and HighCrit temperature thresholds, respectively, for the CPU Die.

If the CPU Die temperature value reaches the HighWarn (75°C/167°F) and HighCrit (85°C/185°F) levels, warning and critical messages, respectively, are issued.

If the value reaches 75°C/167°F or greater, you receive a warning message indicating HighWarn. The system continues to operate, but operator action is recommended to bring the system back to a normal state.

If the value reaches 85°C/185°F or greater, you receive a critical (HighCrit) message instead, that indicates the system continues to operate, but the system is approaching shutdown.

Note Beware if the temperature reaches or exceeds 100°C/212°F, which is the HighShut value, a Shutdown message is issued and the CPU Die area shuts down.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System shutdown for NPE Inlet is 80C/176F</td>
<td>This is the HighShut temperature threshold for the NPE Inlet. If the temperature reaches or exceeds 80C/176F, a Shutdown message is issued and the NPE Inlet area is shut down.</td>
</tr>
<tr>
<td>System shutdown for NPE Outlet is 84C/183F</td>
<td>This is the HighShut temperature threshold for the NPE Outlet. If the temperature reaches or exceeds 84C/183F, a Shutdown message is issued and the NPE Outlet area is shut down.</td>
</tr>
<tr>
<td>System shutdown for CPU Die is 100C/212F</td>
<td>This is the HighShut temperature threshold for the CPU Die. If the temperature reaches or exceeds 100C/212F, a Shutdown message is issued and the CPU Die area is shut down.</td>
</tr>
</tbody>
</table>
| +3.30 V +2.30 +3.12 +3.47 +4.29 | The voltage thresholds for the +3.30 V power rail are as follows:  
  • +2.30 is the LowShut voltage threshold.  
  • +3.12 is the LowCrit voltage threshold.  
  • +3.47 is the HighCrit voltage threshold.  
  • +4.29 is the HighShut voltage threshold.  
  
  **Note**  
  The LowWarn and HighWarn voltage levels are not checked and their thresholds are not displayed on the NPE-G2. |
| VDD_CPU +0.89 +1.21 +1.36 +1.71 | The voltage thresholds for the VDD_CPU power rail are as follows:  
  • +0.89 is the LowShut voltage threshold.  
  • +1.21 is the LowCrit voltage threshold.  
  • +1.36 is the HighCrit voltage threshold.  
  • +1.71 is the HighShut voltage threshold.  
  
  **Note**  
  The LowWarn and HighWarn voltage levels are not checked and their thresholds are not displayed on the NPE-G2. |
| VDD_MEM +1.71 +2.34 +2.61 +3.28 | The voltage thresholds for the VDD_MEM power rail are as follows:  
  • +1.71 is the LowShut voltage threshold.  
  • +2.34 is the LowCrit voltage threshold.  
  • +2.61 is the HighCrit voltage threshold.  
  • +3.28 is the HighShut voltage threshold.  
  
  **Note**  
  The LowWarn and HighWarn voltage levels are not checked and their thresholds are not displayed on the NPE-G2. |
The voltage thresholds for the VTT power rail are as follows:

- +0.85 is the LowShut voltage threshold.
- +1.17 is the LowCrit voltage threshold.
- +1.32 is the HighCrit voltage threshold.
- +1.64 is the HighShut voltage threshold.

Note: The LowWarn and HighWarn voltage levels are not checked and their thresholds are not displayed on the NPE-G2.

Cisco 7000 Series Routers

The following are examples of messages that display on the system console when a measurement has exceeded an acceptable margin:

ENVIRONMENTAL WARNING: Air flow appears marginal.
ENVIRONMENTAL WARNING: Internal temperature measured 41.3°C
ENVIRONMENTAL WARNING: +5 volt testpoint measured 5.310(V)

The system displays the following message if voltage or temperature exceed maximum margins:

SHUTDOWN: air flow problem

In the following example, there have been two intermittent power failures since a router was turned on, and the lower power supply is not functioning. The last intermittent power failure occurred on Monday, June 10, 1996, at 11:07 p.m.

```
7000# show environment all
Environmental Statistics
   Environmental status as of 23:19:47 UTC Wed Jun 12 1996
   Data is 6 second(s) old, refresh in 54 second(s)
   WARNING: Lower Power Supply is NON-OPERATIONAL
   Lower Power Supply:700W, OFF       Upper Power Supply: 700W, ON
   Intermittent Powerfail(s): 2       Last on 23:07:05 UTC Mon Jun 10 1996
   +12 volts measured at 12.05(V)     
   +5 volts measured at 4.96(V)       
   -12 volts measured at -12.05(V)    
   +24 volts measured at 23.80(V)     
   Airflow temperature measured at 38(C)
   Inlet temperature measured at 25(C)
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental status as of...</td>
<td>Date and time of last query.</td>
</tr>
<tr>
<td>Data is..., refresh in...</td>
<td>Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.</td>
</tr>
</tbody>
</table>
If environmental measurements are not within specification, warning messages are displayed.

WARNING: Lower Power Supply Type of power supply installed and its status (on or off).

Upper Power Supply Type of power supply installed and its status (on or off).

Intermittent Powerfail(s) Number of power hits (not resulting in shutdown) since the system was last booted.

Voltage specifications System voltage measurements.

Airflow and inlet temperature Temperature of air coming in and going out.

The following example is for the Cisco 7000 series routers. The router retrieves the environmental statistics at the time of the last shutdown. In this example, the last shutdown was Friday, May 19, 1995, at 12:40 p.m., so the environmental statistics at that time are displayed.

Router# show environment last
Environmental Statistics
Environmental status as of 14:47:00 UTC Sun May 21 1995
Data is 6 second(s) old, refresh in 54 second(s)
WARNING: Upper Power Supply is NON-OPERATIONAL
LAST Environmental Statistics
Environmental status as of 12:40:00 UTC Fri May 19 1995
Lower Power Supply: 700W, ON Upper Power Supply: 700W, OFF
No Intermittent Powerfails
+12 volts measured at 12.05(V)
+5 volts measured at 4.98(V)
+12 volts measured at -12.00(V)
+24 volts measured at 23.80(V)
Airflow temperature measured at 30(C)
Inlet temperature measured at 23(C)

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

**Table 69: show environment last Field Descriptions for the Cisco 7000 Series Routers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental status as of...</td>
<td>Date and time of last query.</td>
</tr>
<tr>
<td>Data is..., refresh in...</td>
<td>Environmental measurements are output into a buffer every 60 seconds,</td>
</tr>
<tr>
<td></td>
<td>unless other higher-priority processes are running.</td>
</tr>
<tr>
<td>WARNING:</td>
<td>If environmental measurements are not within specification, warning</td>
</tr>
<tr>
<td></td>
<td>messages are displayed.</td>
</tr>
<tr>
<td>LAST Environmental Statistics</td>
<td>Displays test point values at time of the last environmental shutdown.</td>
</tr>
<tr>
<td>Lower Power Supply</td>
<td>For the Cisco 7000 router, indicates the status of the two 700W power</td>
</tr>
<tr>
<td>Upper Power Supply</td>
<td>supplies.</td>
</tr>
<tr>
<td></td>
<td>For the Cisco 7010 router, indicates the status of the single 600W power</td>
</tr>
<tr>
<td></td>
<td>supply.</td>
</tr>
</tbody>
</table>
The following example shows sample output for the current environmental status in tables that list voltage and temperature parameters. There are three warning messages: one each about the lower power supply, the airflow temperature, and the inlet temperature. In this example, voltage parameters are shown to be in the normal range, airflow temperature is at a critical level, and inlet temperature is at the warning level.

Router> `show environment table`

Environmental Statistics
Environmental status as of Mon 11-2-1992 17:43:36
Data is 52 second(s) old, refresh in 8 second(s)
WARNING: Lower Power Supply is NON-OPERATIONAL
WARNING: Airflow temperature has reached CRITICAL level at 73°C
WARNING: Inlet temperature has reached WARNING level at 41°C

Voltage Parameters:

<table>
<thead>
<tr>
<th></th>
<th>CRITICAL</th>
<th>NORMAL</th>
<th>CRITICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>+12(V)</td>
<td>10.20</td>
<td>12.05(V)</td>
<td>13.80</td>
</tr>
<tr>
<td>+5(V)</td>
<td>4.74</td>
<td>4.98(V)</td>
<td>5.26</td>
</tr>
<tr>
<td>-12(V)</td>
<td>-10.20</td>
<td>-12.05(V)</td>
<td>-13.80</td>
</tr>
<tr>
<td>+24(V)</td>
<td>20.00</td>
<td>24.00(V)</td>
<td>28.00</td>
</tr>
</tbody>
</table>

Temperature Parameters:

<table>
<thead>
<tr>
<th></th>
<th>WARNING</th>
<th>NORMAL</th>
<th>WARNING</th>
<th>CRITICAL</th>
<th>SHUTDOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airflow</td>
<td>10</td>
<td>60</td>
<td>70</td>
<td>73°C</td>
<td>88</td>
</tr>
<tr>
<td>Inlet</td>
<td>10</td>
<td>39</td>
<td>41°C</td>
<td>46</td>
<td>64</td>
</tr>
</tbody>
</table>

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

### Table 70: show environment table Field Descriptions for the Cisco 7000 Series Routers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SENSE (Voltage Parameters)</td>
<td>Voltage specification for a DC line.</td>
</tr>
<tr>
<td>SENSE (Temperature Parameters)</td>
<td>Air being measured. Inlet measures the air coming in, and Airflow measures the temperature of the air inside the chassis.</td>
</tr>
<tr>
<td>WARNING</td>
<td>System is approaching an out-of-tolerance condition.</td>
</tr>
<tr>
<td>NORMAL</td>
<td>All monitored conditions meet normal requirements.</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Out-of-tolerance condition exists.</td>
</tr>
<tr>
<td>SHUTDOWN</td>
<td>Processor has detected condition that could cause physical damage to the system.</td>
</tr>
</tbody>
</table>

### Cisco 7200 Series Routers

The system displays the following message if the voltage or temperature enters the “Warning” range:

`%ENVM-4-ENWWARN: Chassis outlet 3 measured at 55C/131F`

The system displays the following message if the voltage or temperature enters the “Critical” range:

`%ENVM-2-ENVCRT: +3.45 V measured at +3.65 V`
The system displays the following message if the voltage or temperature exceeds the maximum margins:

%ENVM-0-SHUTDOWN: Environmental Monitor initiated shutdown

The following message is sent to the console if a power supply has been inserted or removed from the system. This message relates only to systems that have two power supplies.

%ENVM-6-PSCHANGE: Power Supply 1 changed from Zytek AC Power Supply to removed

The following message is sent to the console if a power supply has been powered on or off. In the case of the power supply being shut off, this message can be due to the user shutting off the power supply or to a failed power supply. This message relates only to systems that have two power supplies.

%ENVM-6-PSLEV: Power Supply 1 state changed from normal to shutdown

The following is sample output from the `show environment all` command on the Cisco 7200 series routers when there is a voltage warning condition in the system:

```
7200# show environment all
Power Supplies:
   Power supply 1 is unknown. Unit is off.
   Power supply 2 is Zytek AC Power Supply. Unit is on.
Temperature readings:
   chassis inlet measured at 25C/77F
   chassis outlet 1 measured at 29C/84F
   chassis outlet 2 measured at 36C/96F
   chassis outlet 3 measured at 44C/111F
Voltage readings:
   +3.45 V measured at +3.83 V: Voltage in Warning range!
   +5.15 V measured at +5.09 V
   +12.15 measured at +12.42 V
   -11.95 measured at -12.10 V
```

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

**Table 71: show environment all Field Descriptions for the Cisco 7200 Series Router**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supplies</td>
<td>Current condition of the power supplies including the type and whether the power supply is on or off.</td>
</tr>
<tr>
<td>Temperature readings</td>
<td>Current measurements of the chassis temperature at the inlet and outlet locations.</td>
</tr>
<tr>
<td>Voltage readings</td>
<td>Current measurement of the power supply test points.</td>
</tr>
</tbody>
</table>

The following example is for the Cisco 7200 series routers. This example shows the measurements immediately before the last shutdown and the reason for the last shutdown (if appropriate).

```
7200# show environment last
   chassis inlet     previously measured at 27C/80F
   chassis outlet 1  previously measured at 31C/87F
   chassis outlet 2  previously measured at 37C/98F
   chassis outlet 3  previously measured at 45C/113F
   +3.3 V            previously measured at 4.02
   +5.0 V            previously measured at 4.92
   +12.0 V           previously measured at 12.65
```
The following table describes the significant fields shown in the display.

**Table 72: show environment Last Field Descriptions for the Cisco 7200 Series Router**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis inlet</td>
<td>Temperature measurements at the inlet area of the chassis.</td>
</tr>
<tr>
<td>chassis outlet</td>
<td>Temperature measurements at the outlet areas of the chassis.</td>
</tr>
<tr>
<td>voltages</td>
<td>Power supply test point measurements.</td>
</tr>
<tr>
<td>last shutdown reason</td>
<td>Possible shutdown reasons are power supply shutdown, critical temperature, and</td>
</tr>
<tr>
<td></td>
<td>critical voltage.</td>
</tr>
</tbody>
</table>

The following example is for the Cisco 7200 series routers. This information lists the temperature and voltage shutdown thresholds for each sensor.

7200# show environment table

<table>
<thead>
<tr>
<th>Sample Point</th>
<th>LowCritical</th>
<th>LowWarning</th>
<th>HighWarning</th>
<th>HighCritical</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis inlet</td>
<td>40C/104F</td>
<td>50C/122F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chassis outlet 1</td>
<td>43C/109F</td>
<td>53C/127F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chassis outlet 2</td>
<td>75C/167F</td>
<td>75C/167F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chassis outlet 3</td>
<td>55C/131F</td>
<td>65C/149F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+3.45 V</td>
<td>+2.76</td>
<td>+3.10</td>
<td>+3.80</td>
<td>+4.14</td>
</tr>
<tr>
<td>+5.15 V</td>
<td>+4.10</td>
<td>+4.61</td>
<td>+5.67</td>
<td>+6.17</td>
</tr>
<tr>
<td>+12.15 V</td>
<td>+9.72</td>
<td>+10.91</td>
<td>+13.37</td>
<td>+14.60</td>
</tr>
<tr>
<td>Shutdown system at 70C/158F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Table 73: show environment Table Field Descriptions for the Cisco 7200 Series Router**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Point</td>
<td>Area for which measurements are taken.</td>
</tr>
<tr>
<td>LowCritical</td>
<td>Level at which a critical message is issued for an out-of-tolerance voltage condition.</td>
</tr>
<tr>
<td></td>
<td>The system continues to operate; however, the system is approaching shutdown.</td>
</tr>
<tr>
<td>LowWarning</td>
<td>Level at which a warning message is issued for an out-of-tolerance voltage condition.</td>
</tr>
<tr>
<td></td>
<td>The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>HighWarning</td>
<td>Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>HighCritical</td>
<td>Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.</td>
</tr>
<tr>
<td>Shutdown system at</td>
<td>The system is shut down if the specified temperature is met.</td>
</tr>
</tbody>
</table>
Cisco 7500 Series Routers

The sample output for the Cisco 7500 series routers may vary depending on the specific model (for example, the Cisco 7513 router). The following is sample output from the `show environment all` command on the Cisco 7500 series routers:

```
7500# show environment all
Arbiter type 1, backplane type 7513 (id 2)
Power supply #1 is 1200W AC (id 1), power supply #2 is removed (id 7)
Active fault conditions: none
Fan transfer point: 100%
Active trip points: Restart_Inhibit
15 of 15 soft shutdowns remaining before hard shutdown

Dbus slots: X XX X
card inlet hotspot exhaust
RSP(6) 35C/95F 47C/116F 40C/104F
RSP(7) 35C/95F 43C/109F 39C/102F
Shutdown temperature source is 'hotpoint' on RSP(6), requested RSP(6)
+12V measured at 12.31
+5V measured at 5.21
-12V measured at -12.07
+24V measured at 22.08
+2.5 reference is 2.49
PS1 +5V Current measured at 59.61 A (capacity 200 A)
PS1 +12V Current measured at 5.08 A (capacity 35 A)
PS1 -12V Current measured at 0.42 A (capacity 3 A)
PS1 output is 378 W
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbiter type 1</td>
<td>Numbers indicating the arbiter type and backplane type.</td>
</tr>
<tr>
<td>Power supply</td>
<td>Number and type of power supply installed in the chassis.</td>
</tr>
<tr>
<td>Active fault conditions</td>
<td>Lists any fault conditions that exist (such as power supply failure, fan failure, and temperature too high).</td>
</tr>
<tr>
<td>Fan transfer point</td>
<td>Software-controlled fan speed. If the router is operating below its automatic restart temperature, the transfer point is reduced by 10 percent of the full range each minute. If the router is at or above its automatic restart temperature, the transfer point is increased in the same way.</td>
</tr>
<tr>
<td>Active trip points</td>
<td>Compares temperature sensor against the values displayed at the bottom of the <code>show environment</code> table command output.</td>
</tr>
</tbody>
</table>
When the temperature increases above the “board shutdown” level, a soft shutdown occurs (that is, the cards are shut down, and the power supplies, fans, and CI continue to operate). When the system cools to the restart level, the system restarts. The system counts the number of times this occurs and keeps the up/down cycle from continuing forever. When the counter reaches zero, the system performs a hard shutdown, which requires a power cycle to recover. The soft shutdown counter is reset to its maximum value after the system has been up for 6 hours.

**Dbus slots:**
Indicates which chassis slots are occupied.

**card, inlet, hotspot, exhaust**
Temperature measurements at the inlet, hotspot, and exhaust areas of the card. The (6) and (7) indicate the slot numbers. Dual Route Switch Processor (RSP) chassis can show two RSPs.

**Shutdown temperature source**
Indicates which of the three temperature sources is selected for comparison against the “shutdown” levels listed with the `show environment table` command.

**Voltages (+12V, +5V, -12V, +24V, +2.5)**
Voltages measured on the backplane.

**PS1**
Current measured on the power supply.

The following example is for the Cisco 7500 series routers. This example shows the measurements immediately before the last shutdown.

```
7500# show environment last
RSP(4) Inlet previously measured at 37C/98F
RSP(4) Hotpoint previously measured at 46C/114F
RSP(4) Exhaust previously measured at 52C/125F
+12 Voltage previously measured at 12.26
+5 Voltage previously measured at 5.17
-12 Voltage previously measured at -12.03
+24 Voltage previously measured at 23.78
```

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

**Table 75: show environment last Field Descriptions for the Cisco 7500 Series Routers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSP(4) Inlet, Hotpoint, Exhaust</td>
<td>Temperature measurements at the inlet, hotspot, and exhaust areas of the card.</td>
</tr>
<tr>
<td>Voltages</td>
<td>Voltages measured on the backplane.</td>
</tr>
</tbody>
</table>

The following example is for the Cisco 7500 series router. This information lists the temperature and voltage thresholds for each sensor. These thresholds indicate when error messages occur. There are two level of messages: warning and critical.

```
7500# show environment table
Sample Point LowCritical LowWarning HighWarning HighCritical
```

Cisco IOS Configuration Fundamentals Command Reference
RSP(4) Inlet 44C/111F 50C/122F  
RSP(4) Hotpoint 54C/129F 60C/140F  
RSP(4) Exhaust  
+12 Voltage 10.90 11.61 12.82 13.38  
+5 Voltage 4.61 4.94 5.46 5.70  
-12 Voltage -10.15 -10.76 -13.25 -13.86  
+24 Voltage 20.38 21.51 26.42 27.65  
2.5 Reference 2.43 2.51  
Shutdown boards at 70C/158F  
Shutdown power supplies at 76C/168F  
Restart after shutdown below 40C/104F

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

Table 76: show environment Field Descriptions for the Cisco 7500 Series Routers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Point</td>
<td>Area for which measurements are taken.</td>
</tr>
<tr>
<td>LowCritical</td>
<td>Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.</td>
</tr>
<tr>
<td>LowWarning</td>
<td>Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>HighWarning</td>
<td>Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>HighCritical</td>
<td>Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.</td>
</tr>
<tr>
<td>Shutdown boards at</td>
<td>The card is shut down if the specified temperature is met.</td>
</tr>
<tr>
<td>Shutdown power supplies at</td>
<td>The system is shut down if the specified temperature is met.</td>
</tr>
<tr>
<td>Restart after shutdown</td>
<td>The system will restart when the specified temperature is met.</td>
</tr>
</tbody>
</table>

Cisco AS5300 Series Access Servers

In the following example, keywords and options are limited according to the physical characteristics of the system is shown:

as5300# show environment ?
  all  All environmental monitor parameters
  last Last environmental monitor parameters
  table Temperature and voltage ranges
| Output modifiers
<cr>
as5300# show environment table
%This option not available on this platform
Cisco 12000 Series GSRs

The following examples are for the Cisco 12000 series GSRs.

The following is sample output from the `show environment` command for a Cisco 12012 router. Slots 0 through 11 are the line cards, slots 16 and 17 are the clock and scheduler cards, slots 18 through 20 are the switch fabric cards, slots 24 through 26 are the power supplies, and slots 28 and 29 are the blowers. An “NA” in the table means that no values were returned. In some cases it is because the equipment is not supported for that environmental parameter (for example, the power supply and blowers in slots 24, 26, 28, and 29 do not have a 3V power supply, so an NA is displayed).

```
Router# show environment
Slot # 3V  5V  MBUS  5V  Hot Sensor  Inlet Sensor
     (mv) (mv)  (mv)  (deg C)  (deg C)
 0    3300 4992 5040  42.0    37.0
 2    3296 4976 5136  40.0    33.0
 4    3280 4992 5120  38.5    31.5
 7    3280 4984 5136  42.0    32.0
 9    3292 4968 5160  39.5    31.5
 11   3288 4992 5152  40.0    30.5
 16   3308 NA  5056  42.5    38.0
 17   3292 NA  5056  40.5    36.5
 18   3304 NA  5176  36.5    35.0
 19   3300 NA  5184  37.5    33.5
 20   3304 NA  5168  36.5    34.0
 24   NA   5536 5120  NA    31.5
 26   NA   5544 5128  NA    31.5
 28   NA   NA  5128  NA    NA
 29   NA   NA  5104  NA    NA

Slot # 48V AMP_48
     (Volt) (Amp)
 24   46   12
 26   46   19

Slot # Fan 0 Fan 1 Fan 2
     (RPM) (RPM) (RPM)
 28 2160 2190 2168
 29 2130 2190 2070
```

The following table describes the significant fields shown and lists the equipment supported by each environmental parameter. “NA” indicates that the reading could not be obtained, so the command should be run again.

**Table 77: show environment Field Descriptions for the Cisco 12000 Series Routers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot #</td>
<td>Slot number of the equipment. On the Cisco 12012 router, slots 0 through 11 are the line cards, slots 16 and 17 are the clock and scheduler cards, slots 18 through 20 are the switch fabric cards, slots 24 through 27 are the power supplies, and slots 28 and 29 are the blowers.</td>
</tr>
<tr>
<td>3V (mv)</td>
<td>Measures the 3V power supply on the card. The 3V power supply is on the line cards, GRP card, clock and scheduler cards, and switch fabric cards.</td>
</tr>
<tr>
<td>5V (mv)</td>
<td>Measures the 5V power supply on the card. The 5V power supply is on the line cards, GRP card, and power supplies.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBUS 5V (mv)</td>
<td>Measures the 5V MBus on the card. The 5V MBus is on all equipment.</td>
</tr>
<tr>
<td>Hot Sensor (deg C)</td>
<td>Measures the temperature at the hot sensor on the card. The hot sensor is on the line cards, GRP card, clock and scheduler cards, switch fabric cards, and blowers.</td>
</tr>
<tr>
<td>Inlet Sensor (deg C)</td>
<td>Measures the current inlet temperature on the card. The inlet sensor is on the line cards, GRP card, clock and scheduler cards, switch fabric cards, and power supplies.</td>
</tr>
<tr>
<td>48V (Volt)</td>
<td>Measures the DC power supplies.</td>
</tr>
<tr>
<td>AMP_48 (Amp)</td>
<td>Measures the AC power supplies.</td>
</tr>
<tr>
<td>Fan 0, Fan 1, Fan 2 (RPM)</td>
<td>Measures the fan speed in rotations per minute.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show environment all` command for the Cisco 12008 router. Slots 0 through 7 are the line cards, slots 16 and 17 are the clock scheduler cards (the clock scheduler cards control the fans), slots 18 through 20 are the switch fabric cards, and slots 24 and 26 are the power supplies. The Cisco 12008 router does not support slots 25, 27, 28, and 29. An “NA” in the table means that no values were returned. In some cases it is because the equipment is not supported for that environmental parameter (for example, the power supplies in slots 24 and 26 do not have a hot sensor, so an NA is displayed).

```
Router# show environment all
Slot # Hot Sensor Inlet Sensor
       (deg C)  (deg C)
 2    31.0   22.0
 5    33.5   26.5
 16   25.5   21.5
 18   22.0   21.0
 19   22.5   21.0
 24   NA    29.5
 26   NA    24.5
Slot # 3V 5V MBUS 5V
       (mv) (mv) (mv)
 2   3292  5008  5136
 5   3292  5000  5128
 16  3272  NA    5128
 18  3300  NA    5128
 19  3316  NA    5128
Slot # 5V MBUS 5V 48V AMP_48
       (mv) (mv) (Volt) (Amp)
 24   0    5096  3    0
 26  5544  5144  47   3
Slot # Fan Information
 16 Voltage 16V Speed slow: Main Fans Ok Power Supply fans Ok
Alarm Indicators
  No alarms
Slot # Card Specific Leds
 16 Mbus OK SFCs Failed
 18 Mbus OK
 19 Mbus OK
 24 Input Failed
 26 Input Ok
```

The following is sample output from the `show environment table` command for a Cisco 12012 router. The `show environment table` command lists the warning, critical, and shutdown limits on
your system and includes the GRP card and line cards (slots 0 to 15), clock and scheduler cards (slots 16 and 17), switch fabric cards (slots 18 to 20), and blowers.

Router# **show environment table**

<table>
<thead>
<tr>
<th>Hot Sensor Temperature Limits (deg C):</th>
<th>Warning</th>
<th>Critical</th>
<th>Shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP/GLC (Slots 0-15)</td>
<td>40</td>
<td>46</td>
<td>57</td>
</tr>
<tr>
<td>CSC (Slots 16-17)</td>
<td>46</td>
<td>51</td>
<td>65</td>
</tr>
<tr>
<td>SFC (Slots 18-20)</td>
<td>41</td>
<td>46</td>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inlet Sensor Temperature Limits (deg C):</th>
<th>Warning</th>
<th>Critical</th>
<th>Shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP/GLC (Slots 0-15)</td>
<td>35</td>
<td>40</td>
<td>52</td>
</tr>
<tr>
<td>CSC (Slots 16-17)</td>
<td>40</td>
<td>45</td>
<td>59</td>
</tr>
<tr>
<td>SFC (Slots 18-20)</td>
<td>37</td>
<td>42</td>
<td>54</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3V Ranges (mv):</th>
<th>Warning Below</th>
<th>Critical Above</th>
<th>Shutdown Below</th>
<th>Above</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP/GLC (Slots 0-15)</td>
<td>3200</td>
<td>3400</td>
<td>3100</td>
<td>3500</td>
</tr>
<tr>
<td>CSC (Slots 16-17)</td>
<td>3200</td>
<td>3400</td>
<td>3100</td>
<td>3500</td>
</tr>
<tr>
<td>SFC (Slots 18-20)</td>
<td>3200</td>
<td>3400</td>
<td>3100</td>
<td>3500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5V Ranges (mv):</th>
<th>Warning Below</th>
<th>Critical Above</th>
<th>Shutdown Below</th>
<th>Above</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP/GLC (Slots 0-15)</td>
<td>4850</td>
<td>5150</td>
<td>4750</td>
<td>5250</td>
</tr>
<tr>
<td>CSC (Slots 16-17)</td>
<td>4820</td>
<td>5150</td>
<td>4720</td>
<td>5250</td>
</tr>
<tr>
<td>SFC (Slots 17-20)</td>
<td>5000</td>
<td>5250</td>
<td>4900</td>
<td>5350</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MBUS_5V Ranges (mv):</th>
<th>Warning Below</th>
<th>Critical Above</th>
<th>Shutdown Below</th>
<th>Above</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP/GLC (Slots 0-15)</td>
<td>5000</td>
<td>5250</td>
<td>4900</td>
<td>5350</td>
</tr>
<tr>
<td>CSC (Slots 16-17)</td>
<td>4820</td>
<td>5150</td>
<td>4720</td>
<td>5250</td>
</tr>
<tr>
<td>SFC (Slots 17-20)</td>
<td>5000</td>
<td>5250</td>
<td>4900</td>
<td>5350</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blower Operational Range (RPM):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Blower:</td>
</tr>
<tr>
<td>Warning Below</td>
</tr>
<tr>
<td>Fan 0</td>
</tr>
<tr>
<td>Fan 1</td>
</tr>
<tr>
<td>Fan 2</td>
</tr>
</tbody>
</table>

| Bottom Blower:               |
| Warning Below | Critical Below |
| Fan 0 | 1000 | 750 |
| Fan 1 | 1000 | 750 |
| Fan 2 | 1000 | 750 |

The following is sample output from the **show environment leds** command for a Cisco 12012 router. The **show environment leds** command lists the status of the MBus LEDs on the clock, scheduler, and the switch fabric cards.

Router# **show environment leds**

16 leds MBus OK
18 leds MBus OK
19 leds MBus OK
20 leds MBus OK
Cisco 7304 Router

The following is sample output from the `show environment all` command on a Cisco 7304 router with modular services cards (MSCs) and shared port adapters (SPAs) installed:

```
Router# show environment all
Power Supplies:
    Power supply 1 is AC power supply. Unit is on.
    Power supply 2 is empty.
Fans:
    Fan 1 is on.
    Fan 2 is on.
Temperature readings:
    Active RP (NPEG100, slot 0):
        npeg100 outlet measured at 29C/84F
        npeg100 inlet measured at 34C/93F
        npeg100 hotspot measured at 35C/95F
    Line card (7304-MSC-100, slot 4):
        7304-MSC-100 measured at 32C/89F
    Card in subslot 4/0:
        SPA-4FE-7304 inlet measured at 31C/87F
        SPA-4FE-7304 outlet measured at 32C/89F
Voltage readings:
    Active RP (NPEG100, slot 0):
        npe outlet 2.5 V measured at 2.496 V
        npe outlet 3.3 V measured at 3.302 V
        npe outlet 5.0 V measured at 4.992 V
        npe outlet 12.0 V measured at 11.812 V
        npe outlet 3.3c V measured at 3.199 V
        npe inlet 1.5 V measured at 1.494 V
        npe outlet 1.8 V measured at 1.790 V
        npe outlet 1.2 V measured at 1.198 V
        npe outlet 1.2c V measured at 1.198 V
    Line card (7304-MSC-100, slot 4):
        7304-MSC-100 0.75 V measured at 0.733 V
        7304-MSC-100 1.5 V measured at 1.494 V
        7304-MSC-100 2.5 V measured at 2.483 V
        7304-MSC-100 3.3 V measured at 3.250 V
        7304-MSC-100 12 V measured at 11.937 V
    Card in subslot 4/0:
        SPA-4FE-7304 1.8V measured at 1.802 V
        SPA-4FE-7304 1.5V measured at 1.503 V
        SPA-4FE-7304 2.5V measured at 2.474 V
        SPA-4FE-7304 3.3V measured at 3.252 V
        SPA-4FE-7304 1.0V measured at 1.015 V
Envm stats saved 13 time(s) since reload
```

The following is sample output from the `show environment last` command on a Cisco 7304 router with MSCs and SPAs installed and an NSE-100:

```
Router# show environment last
Temperature information:
    NSE board:
        nse outlet is unmeasured
        nse inlet is unmeasured
        nse hotspot is unmeasured
        nse db is unmeasured
    Line card slot 4:
        7304-MSC-100 is unmeasured
    Card in subslot 4/1:
        SPA-4FE-7304 inlet previously measured at 30C/86F
```

The following is sample output from the `show environment table` command on a Cisco 7304 router with MSCs and SPAs installed:

**Temperature tables:**
- **Active RP (NPEG100, slot 0):**
  - Sample Point
  - NPEG outlet 53°C/127°F 68°C/154°F 73°C/163°F
  - NPEG inlet 53°C/127°F 68°C/154°F 73°C/163°F
  - NPEG hotspot 53°C/127°F 68°C/154°F 73°C/163°F
- **Line card (7304-MSC-100, slot 4):**
  - Sample Point
  - 7304-MSC outlet 48°C/118°F 63°C/145°F 68°C/154°F
  - 7304-MSC inlet 53°C/127°F 68°C/154°F 73°C/163°F
- **Card in subslot 4/0:**
  - Sample Point
  - SPA-4FE inlet 52°C/125°F 67°C/152°F 72°C/161°F
  - SPA-4FE outlet 52°C/125°F 67°C/152°F 72°C/161°F

**Voltage tables:**
- **Active RP (NPEG100, slot 0):**
  - Sample Point
  - NPE outlet 2.5 V 2.275 V 2.375 V 2.400 V 2.600 V 2.625 V 2.725 V
  - NPE outlet 5.0 V 4.500 V 4.750 V 4.800 V 5.200 V 5.250 V 5.500 V
  - NPE inlet 1.5 V 1.350 V 1.425 V 1.455 V 1.545 V 1.575 V 1.650 V
  - NPE inlet 1.8 V 1.620 V 1.710 V 1.728 V 1.872 V 1.890 V 1.980 V
  - NPE inlet 1.2 V 1.128 V 1.164 V 1.167 V 1.233 V 1.236 V 1.272 V
  - NPE inlet 1.2c V 1.128 V 1.164 V 1.167 V 1.233 V 1.236 V 1.272 V
- **Line card (7304-MSC-100, slot 4):**
  - Sample Point
  - 7304-MSC outlet 0.75 V 0.559 V 0.600 V 0.600 V 0.900 V 0.900 V 0.941 V
  - 7304-MSC outlet 1.5 V 1.350 V 1.440 V 1.455 V 1.545 V 1.560 V 1.650 V
  - 7304-MSC outlet 2.5 V 2.250 V 2.375 V 2.400 V 2.600 V 2.625 V 2.750 V
Cisco uBR10012 Router

The following is sample output from the `show environment subslot slot/subslot` command on a Cisco uBR10012 router:

```
Router# show environment subslot 7/0
------------------------------------------------------------------------
TEMPERATURE/POWER INFORMATION
------------------------------------------------------------------------
Number of Temperature Sensors : 11
Sampling frequency : 2 minutes
------------------------------------------------------------------------
Sensor | ID | Current | Minor | Major | Critical | Alarm | | | Temperature | Threshold | Condition |
------------------------------------------------------------------------

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

Table 78: `show environment` table Field Descriptions for the Cisco 7304 Router

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Point</td>
<td>Area for which measurements are taken.</td>
</tr>
<tr>
<td>LowShut</td>
<td>Lowest level for an out-of-tolerance condition at which the system shuts itself down. For out-of-tolerance conditions with SPA environment variables, only the SPA is shut down.</td>
</tr>
<tr>
<td>LowCrit/LowCritical</td>
<td>Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.</td>
</tr>
<tr>
<td>LowWarn/LowWarning</td>
<td>Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>HighWarn/HighWarning</td>
<td>Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.</td>
</tr>
<tr>
<td>HighCrit/HighCritical</td>
<td>Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.</td>
</tr>
<tr>
<td>HighShut/HighShutdown</td>
<td>Highest level for an out-of-tolerance condition at which the system shuts itself down. For out-of-tolerance conditions with SPA environment variables, only the SPA is shut down.</td>
</tr>
</tbody>
</table>
### Table 79: show environment subslot Field Descriptions for the Cisco uBR10012 Router

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Temperature Sensors</td>
<td>The number of temperature sensors for which measurements are taken.</td>
</tr>
<tr>
<td>Sampling frequency</td>
<td>Temperature sampling frequency.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Sensor name.</td>
</tr>
<tr>
<td>ID</td>
<td>Temperature sensor identifier.</td>
</tr>
<tr>
<td>Current Temperature</td>
<td>Current temperature level.</td>
</tr>
<tr>
<td>Minor</td>
<td>Minor temperature tolerance threshold level.</td>
</tr>
<tr>
<td>Major Threshold</td>
<td>Major temperature tolerance threshold level.</td>
</tr>
<tr>
<td>Critical</td>
<td>Critical temperature tolerance threshold level.</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>Temperature level sampling time.</td>
</tr>
<tr>
<td>Alarm Condition</td>
<td>Alarm state.</td>
</tr>
<tr>
<td>Power Watts</td>
<td>Current power consumption of the router.</td>
</tr>
</tbody>
</table>
### show environment alarm

To display the information about the environmental alarm, use the **show environment alarm** command in user EXEC or privileged EXEC mode.

```
show environment alarm [{status|threshold} [frutype]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>status</strong></td>
<td>(Optional) Displays the operational FRU status.</td>
</tr>
<tr>
<td><strong>threshold</strong></td>
<td>(Optional) Displays the preprogrammed alarm thresholds.</td>
</tr>
<tr>
<td><strong>frutype</strong></td>
<td>(Optional) Alarm type; valid values are <strong>all</strong>, <strong>backplane</strong>, <strong>clock number</strong>, <strong>earl slot</strong>, <strong>fan-tray</strong>, <strong>module slot</strong>, <strong>rp slot</strong>, <strong>power-supply number</strong>, <strong>supervisor slot</strong>, and <strong>vtt number</strong>. See the Note for a list of valid values for <strong>number</strong> and <strong>slot</strong>.</td>
</tr>
</tbody>
</table>

**Command Default**

If you do not enter a **frutype**, all the information about the environmental alarm status is displayed.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Valid values for the **frutype** are as follows:

- **clock number** -- 1 and 2.
- **earl slot** -- See the Note for valid values.
• module slot -- See the Note for valid values.
• rp slot -- See the Note for valid values.
• power-supply number -- 1 and 2.
• supervisor slot -- See the Note for valid values.
• vtt number -- 1 to 3.

Note

The slot argument designates the module and port number. Valid values for slot depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to display all the information about the status of the environmental alarm:

Router>
show environment alarm
threshold
environmental alarm thresholds:
power-supply 1 fan-fail: OK
  threshold #1 for power-supply 1 fan-fail:
    (sensor value != 0) is system minor alarm
power-supply 1 power-output-fail: OK
  threshold #1 for power-supply 1 power-output-fail:
    (sensor value != 0) is system minor alarm
fantray fan operation sensor: OK
  threshold #1 for fantray fan operation sensor:
    (sensor value != 0) is system minor alarm
operating clock count: 2
  threshold #1 for operating clock count:
    (sensor value < 2) is system minor alarm
threshold #2 for operating clock count:
    (sensor value < 1) is system major alarm
operating VTT count: 3
  threshold #1 for operating VTT count:
    (sensor value < 3) is system minor alarm
threshold #2 for operating VTT count:
    (sensor value < 2) is system major alarm
VTT 1 OK: OK
  threshold #1 for VTT 1 OK:
    (sensor value != 0) is system minor alarm
VTT 2 OK: OK
  threshold #1 for VTT 2 OK:
    (sensor value != 0) is system minor alarm
VTT 3 OK: OK
  threshold #1 for VTT 3 OK:
    (sensor value != 0) is system minor alarm
clock 1 OK: OK
  threshold #1 for clock 1 OK:
    (sensor value != 0) is system minor alarm
clock 2 OK: OK
  threshold #1 for clock 2 OK:
    (sensor value != 0) is system minor alarm
module 1 power-output-fail: OK
  threshold #1 for module 1 power-output-fail:
(sensor value != 0) is system major alarm
module 1 outlet temperature: 21C
threshold #1 for module 1 outlet temperature:
(sensor value > 60) is system minor alarm
threshold #2 for module 1 outlet temperature:
(sensor value > 70) is system major alarm
module 1 inlet temperature: 25C
threshold #1 for module 1 inlet temperature:
(sensor value > 60) is system minor alarm
threshold #2 for module 1 inlet temperature:
(sensor value > 70) is system major alarm
module 1 device-1 temperature: 30C
threshold #1 for module 1 device-1 temperature:
(sensor value > 60) is system minor alarm
threshold #2 for module 1 device-1 temperature:
(sensor value > 70) is system major alarm
module 1 device-2 temperature: 29C
threshold #1 for module 1 device-2 temperature:
(sensor value > 60) is system minor alarm
threshold #2 for module 1 device-2 temperature:
(sensor value > 70) is system major alarm
module 5 power-output-fail: OK
threshold #1 for module 5 power-output-fail:
(sensor value != 0) is system major alarm
module 5 outlet temperature: 26C
threshold #1 for module 5 outlet temperature:
(sensor value > 60) is system minor alarm
threshold #2 for module 5 outlet temperature:
(sensor value > 75) is system major alarm
module 5 inlet temperature: 23C
threshold #1 for module 5 inlet temperature:
(sensor value > 50) is system minor alarm
threshold #2 for module 5 inlet temperature:
(sensor value > 65) is system major alarm
EARL 1 outlet temperature: N/O
threshold #1 for EARL 1 outlet temperature:
(sensor value > 60) is system minor alarm
threshold #2 for EARL 1 outlet temperature:
(sensor value > 75) is system major alarm
EARL 1 inlet temperature: N/O
threshold #1 for EARL 1 inlet temperature:
(sensor value > 50) is system minor alarm
threshold #2 for EARL 1 inlet temperature:
(sensor value > 65) is system major alarm

Router>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show environment status</td>
<td>Displays the information about the operational FRU status.</td>
</tr>
<tr>
<td>show environment temperature</td>
<td>Displays the current temperature readings.</td>
</tr>
</tbody>
</table>

### show environment connector

To display the connector rating and power consumption of modules or the backplane, use the `show environment connector` command in user EXEC or privileged EXEC mode.

```
show environment connector [{all|backplane|module number}]
```
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Displays the connector rating of the backplane and the connector rating and power consumption of all modules.</td>
</tr>
<tr>
<td>backplane</td>
<td>(Optional) Displays the connector rating of the backplane.</td>
</tr>
<tr>
<td>module number</td>
<td>(Optional) Displays the connector rating and power consumption of the specified module.</td>
</tr>
</tbody>
</table>

### Command Modes

User EXEC (>) Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXI 4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The output of the `show environment connector` command displays the connector rating of the backplane (chassis) power connector, the connector rating of module connectors, and the power consumption of each installed module.

If your system contains the necessary components for auxiliary power, the auxiliary power connector rating is displayed.

If an installed module contains a voice daughterboard (VDB), the VDB connector rating is displayed.

If you enter the `show environment connector` command with no keywords, the information for the backplane and all modules is displayed.

### Examples

This example shows how to display the connector rating and power consumption of the backplane and all modules:

```
Router>
show environment connector all
chassis connector rating: 1302.00 Watts (31.00 Amps @ 42V)
chassis auxiliary connector rating: 2016.00 Watts (48.00 Amps @ 42V)
module 3
  module 3 connector rating: 1260.00 Watts (30.00 Amps @ 42V)
  module 3 vdb connector rating: 1050.00 Watts (25.00 Amps @ 42V)
  module 3 power consumption: 140.70 Watts (3.35 Amps @ 42V)
module 6
  module 6 connector rating: 1260.00 Watts (30.00 Amps @ 42V)
  module 6 power consumption: 282.24 Watts (6.72 Amps @ 42V)
module 9
  module 9 connector rating: 1260.00 Watts (30.00 Amps @ 42V)
  module 9 auxiliary connector rating: 2016.00 Watts (48.00 Amps @ 42V)
  module 9 vdb connector rating: 1060.00 Watts (25.24 Amps @ 42V)
  module 9 vdb auxiliary rating: 530.00 Watts (12.62 Amps @ 42V)
  module 9 power consumption: 112.56 Watts (2.68 Amps @ 42V)
```

This example shows how to display the connector rating of the backplane:

```
Router>
show environment connector backplane
chassis connector rating: 1302.00 Watts (31.00 Amps @ 42V)
chassis auxiliary connector rating: 2016.00 Watts (48.00 Amps @ 42V)
```
show environment cooling

To display the information about the cooling parameter, use the `show environment cooling` command in user EXEC or privileged EXEC mode.

```
Router> show environment cooling
fan-tray 1:
   fan-tray 1 fan-fail: failed
fan-tray 2:
   fan 2 type: FAN-MOD-9
   fan tray 2 fan-fail: OK
chassis cooling capacity: 690 cfm
ambient temperature: 55C
chassis per slot cooling capacity: 75 cfm
module 1 cooling requirement: 70 cfm
module 2 cooling requirement: 70 cfm
module 5 cooling requirement: 30 cfm
module 6 cooling requirement: 70 cfm
module 8 cooling requirement: 70 cfm
module 9 cooling requirement: 30 cfm
Router>
```
show environment status

To display the information about the operational FRU status, use the `show environment status` command in user EXEC or privileged EXEC mode.

```
show environment status [frutype]
```

**Syntax Description**

- `frutype` (Optional) FRU type; see the Note for a list of valid values.

**Command Default**

If you do not enter a `frutype`, all FRU status information is displayed.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXF</td>
<td>The output of the <code>show environment status power-supply</code> command was changed to include information about the high-capacity power supplies.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Valid values for the `frutype` are as follows:

- `all` -- No arguments.
- `backplane` -- No arguments.
- `clock number` -- 1 and 2.
- `earl slot` -- See the Note for valid values.
- `fan-tray` -- No arguments.
- `module slot` -- See the Note for valid values.
- `power-supply number` -- 1 and 2.
- `rp slot` -- See the Note for valid values.
- `supervisor slot` -- See the Note for valid values.
- `vtt number` -- 1 to 3.

**Note**

The `slot` argument designates the module and port number. Valid values for `slot` depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.
Examples

This example shows how to display the information about the environmental status:

```
Router>
show environment status
backplane:
  operating clock count: 2
  operating VTT count: 3
fan-tray:
  fan-tray fan operation sensor: OK
VTT 1:
  VTT 1 OK: OK
VTT 2:
  VTT 2 OK: OK
VTT 3:
  VTT 3 OK: OK
clock 1:
  clock 1 OK: OK, clock 1 clock-inuse: not-in-use
clock 2:
  clock 2 OK: OK, clock 2 clock-inuse: in-use
power-supply 1:
  power-supply 1 fan-fail: OK
  power-supply 1 power-output-fail: OK
module 1:
  module 1 power-output-fail: OK
  module 1 outlet temperature: 21C
  module 1 inlet temperature: 25C
  module 1 device-1 temperature: 30C
  module 1 device-2 temperature: 29C
EARL 1 outlet temperature: N/O
EARL 1 inlet temperature: N/O
module 5:
  module 5 power-output-fail: OK
  module 5 outlet temperature: 26C
  module 5 inlet temperature: 23C
  module 5 device-1 temperature: 26C
  module 5 device-2 temperature: 27C
Router>
```

This example shows how to display the information about the high-capacity power supplies:

```
Route># show environment status
power-supply 2
power-supply 2:
  power-supply 2 fan-fail: OK
  power-supply 2 power-input 1: none
  power-supply 2 power-input 2: AC low
  power-supply 2 power-input 3: AC high
  power-supply 2 power-input 4: AC high
  power-supply 2 power-output: low (mode 1)
  power-supply 2 power-output-fail: OK
```

The table below describes the fields that are shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operating clock count</td>
<td>Physical clock count.</td>
</tr>
<tr>
<td>operating VTT count</td>
<td>Physical VTT count.</td>
</tr>
</tbody>
</table>
System fan tray failure status. The failure of the system fan tray is indicated as a minor alarm.

Status of the chassis backplane power monitors that are located on the rear of the chassis, under the rear cover. Operation of at least two VTTs is required for the system to function properly. A minor system alarm is signaled when one of the three VTTs fails. A major alarm is signaled when two or more VTTs fail and the supervisor engine is accessible through the console port.

Clock status. Failure of either clock is considered to be a minor alarm.

Fan failure. Fan failures on either or both (if any) power supplies are considered minor alarms.

Power input failure status (none, AC high, AC low).

Power output failure status (high, low).

Exhaust temperature value.

Intake temperature value.

Two devices that measure the internal temperature on each indicated module. The temperature shown indicates the temperature that the device is recording. The devices are not placed at an inlet or an exit but are additional reference points.

### show environment temperature

To display the current temperature readings, use the `show environment temperature` command in user EXEC or privileged EXEC mode.

```
show environment temperature [frutype]
```

**Syntax Description**

```
frutype (Optional) Field replaceable unit (FRU) type; see the “Usage Guidelines” section for a list of valid values.
```

**Command Default**

If you do not enter a `frutype`, the module and EARL temperature readings are displayed.

**Command Modes**

User EXEC Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>
| 12.2(17a)SX   | The `show environment temperature module` command output was updated to include the following information:  
|               | • The name of the ASIC of this sensor.                                     |
|               | • The names of the ASIC are listed if there is more than one ASIC.         |
|               | • The type of sensor is listed if there is more than one sensor on the ASIC.|
|               | • Current temperature.                                                     |
|               | • Major/minor threshold as read in the IDPROM.                             |
|               | • Status of whether the current temperature has exceeded any temperature thresholds. |
| 12.2(17d)SXB  | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA   | This command was integrated into Cisco IOS Release 12.2(33)SRA.             |

Usage Guidelines

Valid values for the `frutype` are as follows:

- `earl slot` -- See the Note below for valid values.
- `module slot` -- See the Note below for valid values.
- `rp slot` -- See the the Note below for valid values.
- `vtt number` -- 1 to 3.
- `clock number` -- 1 and 2.

Note

The `slot` argument designates the module and port number. Valid values for `slot` depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The `show environment temperature module` command output includes the updated information after an SCP response is received.

In the output display, the following applies:

- N/O means not operational--The sensor is broken, returning impossible values.
- N/A means not available--The sensor value is presently not available; try again later.
- VTT 1, 2, and 3 refer to the power monitors that are located on the chassis backplane under the rear cover.

Examples

This example shows how to display the temperature information for a specific module:
Router>
show environment temperature
module 5

module 5 outlet temperature: 34C
module 5 inlet temperature: 27C
module 5 device-1 temperature: 42C
module 5 device-2 temperature: 41C
module 5 asic-1 (SSO-1) temp: 29C
module 5 asic-2 (SSO-2) temp: 29C
module 5 asic-3 (SSO-3) temp: 29C
module 5 asic-4 (SSO-4) temp: 28C
module 5 asic-5 (SSA-1) temp: 29C
module 5 asic-6 (HYPERION-1) temp: 29C

This example shows how to display the temperature readings for all modules:

Router>
show environment temperature
VTT 1 outlet temperature: 25C
VTT 2 outlet temperature: 24C
VTT 3 outlet temperature: 28C
module 1 outlet temperature: 24C
module 1 device-2 temperature: 29C
RP 1 outlet temperature: 25C
RP 1 inlet temperature: 29C
EARL 1 outlet temperature: 25C
EARL 1 inlet temperature: 22C
module 5 outlet temperature: 27C
module 5 inlet temperature: 22C

Router>

The following table describes the fields that are shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outlet temperature</td>
<td>Exhaust temperature value.</td>
</tr>
<tr>
<td>inlet temperature</td>
<td>Intake temperature value.</td>
</tr>
<tr>
<td>device-1 and device-2</td>
<td>Two devices that measure the internal temperature on the indicated module.</td>
</tr>
<tr>
<td>temperature</td>
<td>The temperature shown indicates the temperature that the device is recording.</td>
</tr>
<tr>
<td></td>
<td>The devices are not placed at an inlet or an exit but are additional</td>
</tr>
<tr>
<td></td>
<td>reference points.</td>
</tr>
</tbody>
</table>

Table 81: show environment temperature Command Output Fields
show errdisable detect

To display the error-disable detection status, use the `show errdisable detect` command in user EXEC or privileged EXEC mode.

```
Router> show errdisable detect
ErrDisable Reason                  Detection status
---------------------------------  ----------------
udld                              Enabled
bpduguard                        Enabled
rootguard                        Enabled
packet-buffer-err                 Enabled
pagp-flap                         Enabled
dtp-flap                          Enabled
link-flap                         Enabled
Router#                          
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show environment alarm</code></td>
<td>Displays the information about the environmental alarm.</td>
</tr>
<tr>
<td><code>show environment status</code></td>
<td>Displays the information about the operational FRU status.</td>
</tr>
</tbody>
</table>

**show errdisable detect**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no arguments or keywords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>This command has no default settings.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>User EXEC Privileged EXEC</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was changed to include packet-buffer error status information.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display the error-disable detection status:

```
Router> show errdisable detect
ErrDisable Reason                  Detection status
---------------------------------  ----------------
udld                              Enabled
bpduguard                        Enabled
rootguard                        Enabled
packet-buffer-err                 Enabled
pagp-flap                         Enabled
dtp-flap                          Enabled
link-flap                         Enabled
Router#
```
show errdisable recovery

To display the information about the error-disable recovery timer, use the **show errdisable recovery** command in EXEC mode.

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
This command has no default settings.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display the information about the error-disable recovery timer:

```
Router# show errdisable recovery
ErrDisable Reason  Timer Status
----------------- --------------
udld Enabled
bpduguard Enabled
rootguard Enabled
pagp-flap Enabled
dtp-flap Enabled
link-flap Enabled
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason   Time left(sec)
---------    --------------   ---------------
Fa9/4        link-flap        279
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errdisable recovery</td>
<td>Configures the recovery mechanism variables.</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.</td>
</tr>
</tbody>
</table>

show fastblk

To display fast block memory information, use the **show fastblk** command in privileged EXEC mode.

```
show fastblk [detailed]
```
Syntax Description

- **detailed** *(Optional)* Displays detailed allocated fast block memory pool information.

Command Modes

- Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display allocated fast block memory pool details. When no memory pools are allocated, the “no fastblk memory pools allocated” message is displayed.

Examples

The following is sample output from the `show fastblk` command using the `detailed` keyword. The fields are self-explanatory.

```
Router# show fastblk detailed
Pool name: SCTP ApplReq     flags:DYN_POOL
    total = 400 inuse = 0, free = 400, max = 0
    increment = 200, threshold = 100, hist max = 400
    alloc failures = 0, sub-pool creation failures = 0
    subpool: blks = 0x62966A2C, total = 400, inuse= 0, free = 400
    delete count = 0, flags:
Pool name: SCTP BufSegHdr     flags:DYN_POOL
    total = 9000 inuse = 0, free = 9000, max = 0
    increment = 4500, threshold = 6750, hist max = 9000
    alloc failures = 0, sub-pool creation failures = 0
    subpool: blks = 0x62B8E2F4, total = 9000, inuse= 0, free = 9000
    delete count = 0, flags:
Pool name: SCTP DestAddr     flags:DYN_POOL
    total = 80 inuse = 0, free = 80, max = 0
    increment = 40, threshold = 20, hist max = 80
    alloc failures = 0, sub-pool creation failures = 0
    subpool: blks = 0x62972534, total = 80, inuse= 0, free = 80
    delete count = 0, flags:
Pool name: SCTP Addr     flags:DYN_POOL POOL_HAS_GRWN
    total = 200 inuse = 100, free = 100, max = 0
    increment = 50, threshold = 50, hist max = 200
    alloc failures = 31, sub-pool creation failures = 0
    subpool: blks = 0x6271B6D0, total = 50, inuse= 0, free = 50
    delete count = 0, flags: DYN_SUBPOOL
    subpool: blks = 0x62D8D768, total = 50, inuse= 0, free = 50
    delete count = 0, flags: DYN_SUBPOOL
    subpool: blks = 0x6297680C, total = 100, inuse= 100, free = 0
    delete count = 0, flags:
Pool name: SCTP ChunkDesc     flags:DYN_POOL
    total = 9000 inuse = 0, free = 9000, max = 0
    increment = 4500, threshold = 6750, hist max = 9000
    alloc failures = 0, sub-pool creation failures = 0
    subpool: blks = 0x62B8E6160, total = 1471, inuse= 0, free = 1471
    delete count = 0, flags:
    subpool: blks = 0x62D8D768, total = 7529, inuse= 0, free = 7529
    delete count = 0, flags:
Pool name: SCTP DgramHdr     flags:DYN_POOL
    total = 9000 inuse = 0, free = 9000, max = 0
    increment = 4500, threshold = 6750, hist max = 9000
    alloc failures = 0, sub-pool creation failures = 0
    subpool: blks = 0x62B8E848, total = 9000, inuse= 0, free = 9000
    delete count = 0, flags:
Pool name: SCTP Assoc     flags:DYN_POOL
```

Cisco IOS Configuration Fundamentals Command Reference
show file descriptors

To display a list of open file descriptors, use the **show file descriptors** command in EXEC mode.

**show file descriptors**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

File descriptors are the internal representations of open files. You can use this command to learn if another user has a file open.

**Examples**

The following is sample output from the **show file descriptors** command:

```
Router# show file descriptors
File Descriptors:
   FD  Position  Open  PID  Path
    0  187392   0001  2  tftp://dirt/hampton/c4000-1-m.a
    1  184320   030A  2  flash:/c4000-1-m.a
```

The table below describes the fields shown in the display.

**Table 82: show file descriptors Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD</td>
<td>File descriptor. The file descriptor is a small integer used to specify the file once it has been opened.</td>
</tr>
<tr>
<td>Position</td>
<td>Byte offset from the start of the file.</td>
</tr>
</tbody>
</table>
show file information

To display information about a file, use the `show file information` command in EXEC mode.

```
show file information file-url
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file-url</td>
<td>The URL of the file to display.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show file information` command:

```
Router# show file information tftp://dirt/hampton/c2500-j-l.a
tftp://dirt/hampton/c2500-j-l.a:
  type is image (a.out) [relocatable, run from flash]
  file size is 8624596 bytes, run size is 9044940 bytes [8512316+112248+420344]
  Foreign image
Router# show file information slot0:c7200-js-mz
slot0:c7200-js-mz:
  type is image (elf) []
  file size is 4770316 bytes, run size is 4935324 bytes
  Runnable image, entry point 0x80008000, run from ram
Router1# show file information nvram:startup-config
nvram:startup-config:
  type is ascii text
```

The table below describes the possible file types.

**Table 83: Possible File Types**

<table>
<thead>
<tr>
<th>Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>image (a.out)</td>
<td>Runnable image in a.out format.</td>
</tr>
<tr>
<td>image (elf)</td>
<td>Runnable image in elf format.</td>
</tr>
<tr>
<td>ascii text</td>
<td>Configuration file or other text file.</td>
</tr>
</tbody>
</table>
show file systems

To list available file systems, use the show file systems command in privileged EXEC mode.

```
show file systems
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3AA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was enhanced to display information about the ATA ROM monitor library (monlib) file.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI and the output was modified.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(24)T and the output was modified.</td>
</tr>
<tr>
<td>15.0(01)XO</td>
<td>Note added to explain different byte and usage calculations for show file systems and dir commands on cat4000 series routers.</td>
</tr>
<tr>
<td>15.1(2)SNG</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to learn the alias names, the Prefixes column in the output of the file systems that your router supports.

**Examples**

The following is sample output from the show file systems command:

```
Router# show file systems
File Systems:

Size(b)    Free(b)  Type  Flags  Prefixes
-         -    ram    rw    tmp:
```
The table below describes the significant fields shown in the display.

**Table 84: show file systems Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size(b)</td>
<td>Amount of memory in the file system (in bytes). The &quot;<em>&quot; references the default device/directory when flash is used in a generic manner. For example, if you were to type <code>sh flash</code> and the device actually has <code>bootflash:</code>, the output of <code>sh flash</code> will actually be the output of `dir bootflash: show file systems shows the devices that this rtr can access. The &quot;</em>&quot; indicates the default device.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of free memory in the file system (in bytes).</td>
</tr>
<tr>
<td>Type</td>
<td>Type of file system. The file system can be one of the following types:</td>
</tr>
<tr>
<td></td>
<td>• disk-- The file system is for a rotating medium.</td>
</tr>
<tr>
<td></td>
<td>• flash-- The file system is for a flash memory device.</td>
</tr>
<tr>
<td></td>
<td>• network-- The file system is a network file system (TFTP, rcp, FTP, and so on).</td>
</tr>
<tr>
<td></td>
<td>• nvram-- The file system is for an NVRAM device.</td>
</tr>
<tr>
<td></td>
<td>• opaque-- The file system is a locally generated “pseudo” file system (for example, the “system”) or a download interface, such as brimux.</td>
</tr>
<tr>
<td></td>
<td>• ram-- The file system is for a RAM or EPROM device.</td>
</tr>
<tr>
<td></td>
<td>• tty-- The file system is for a collection of terminal devices.</td>
</tr>
<tr>
<td></td>
<td>• unknown -- The file system is of unknown type.</td>
</tr>
</tbody>
</table>
Permissions for the file system. The file system can have one of the following permission states:

- **ro**—The file system is Read Only.
- **wo**—The file system is Write Only.
- **rw**—The file system is Read/Write.

Prefixes

Alias for the file system. Prefixes marked with a pound symbol (#) indicate a bootable disk.

---

**Note**

As of release 15.0(01)XO, on cat4000 series routers, the `show file systems` and `dir` will display slightly different byte count and usage information for the same file system. This is due to slight difference in how IOS computes these figures for this platform.

### show flh-log

The `show flh-log` command has been replaced by the `more flh:logfile` command. See the description of the `more flh:logfile` command for more information.

### show fm inspect

To display the list and status of the access control lists (ACLs) and ports on which context based access control (CBAC) is configured, use the `show fm inspect` command in user EXEC or privileged EXEC mode.

```
show fm inspect [\{detail|interface type mod|port\}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Displays all of the flow information.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>(Type) Interface type; possible valid values are</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>ethernet, fastetheren, gigabitetheren, tenn Gigbitetheren, port-channel, pos, atm, null, tunnel, and ge-wan</td>
</tr>
<tr>
<td><strong>mod / port</strong></td>
<td>Module and port number.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

If you can configure a VLAN access control list (VACL) on the port before you configure CBAC, the status displayed is INACTIVE; otherwise, it is ACTIVE. If policy feature card (PFC) resources are exhausted, the command displays BRIDGE and is followed by the number of failed currently active NetFlow requests that have been sent to the MSFC2 for processing.

The `show fm inspect` command output includes this information:

- `interface:` -- Interface on which the internet protocol (IP) inspect feature is enabled
- `(direction)` -- Direction in which the IP inspect feature is enabled (IN or OUT)
- `acl name:` -- Name that is used to identify packets being inspected
- `status:` -- (ACTIVE or INACTIVE) displays if HW-assist is provided for this interface+direction (ACTIVE=hardware assisted or INACTIVE)

The optional `detail` keyword displays the ACEs that are part of the ACL that is used for IP inspect on the given interface direction.

**Examples**

This example shows how to display the list and status of CBAC-configured ACLs and ports:

```
Router> show fm inspect
interface:Vlan305(in) status :ACTIVE
  acl name:deny
  interfaces:
    Vlan305(out):status ACTIVE
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show fm summary</code></td>
<td>Displays a summary of FM Information.</td>
</tr>
</tbody>
</table>

**show fm interface**

To display the detailed information about the feature manager on a per-interface basis, use the `show fm interface` command in user EXEC or privileged EXEC mode.

```
show fm interface {interface type mod/port|null |interface-number|port-channel number|vlan vlan-id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type; possible valid values are ethernet, fastethernet, gigabitethernet, tengigabitethernet, port-channel, pos, atm, null, tunnel, and ge-wan</td>
</tr>
<tr>
<td><code>mod / port</code></td>
<td>Module and port number.</td>
</tr>
<tr>
<td><code>null interface-number</code></td>
<td>Specifies the null interface; the valid value is 0.</td>
</tr>
<tr>
<td><code>port-channel number</code></td>
<td>Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.</td>
</tr>
<tr>
<td><code>vlan vlan-id</code></td>
<td>Specifies the virtual local area network (VLAN); valid values are from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.
show fm interface

Command Modes

User EXEC Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17a)SX</td>
<td>The order of the information that is displayed in the <code>show fm interface vlan</code> command output was changed.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `pos`, `atm`, and `ge-wan` keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The `interface-number` argument designates the module and port number. Valid values for `interface-number` depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The `port-channel number` values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the detailed information about the feature manager on a specified interface:

```
Router>

show fm interface fastethernet 2/26
Interface:FastEthernet2/26 IP is enabled
  hw[Egress] = 1, hw[Ingress] = 0
  hw_force_default[Egress] = 0, hw_force_default[Ingress] = 1
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:24
    protocol:ip
    feature #1:
      feature id:FM_IP_ACCESS
      ACL:113
      vmr IP value #1:0, 0, 0, 0, 0, 0, 0, 6 - 1
      vmr IP mask #1:0, 0, FFFF, FFFF, 0, 0, 0, FF
      vmr IP value #2:642D4122, 0, 0, 1, 0, 0, 6 - 1
      vmr IP mask #2:FFFFFFFF, 0, 0, 0, 1, 0, 0, FF
      vmr IP value #3:0, 64020302, 0, 0, 6, 0, 0, 6 - 1
      vmr IP mask #3:0, FFFFFFFF, 0, 0, 6, 0, 0, FF
      vmr IP value #4:0, 64020302, 0, 0, A, 0, 0, 6 - 1
      vmr IP mask #4:0, FFFFFFFF, 0, 0, A, 0, 0, FF
      vmr IP value #5:0, 64020302, 0, 0, 12, 0, 0, 6 - 1
      vmr IP mask #5:0, FFFFFFFF, 0, 0, 12, 0, 0, FF
      vmr IP value #6:0, 0, 0, 0, 0, 0, 0, 0 - 2
      vmr IP mask #6:0, 0, 0, 0, 0, 0, 0, 0
  outbound label:3
    protocol:ip
    feature #1:
      feature id:FM_IP_WCCP
      Service ID:0
```
Service Type: 0

This example shows how to display the detailed information about the feature manager on a specific VLAN:

Router> show fm interface vlan 21
Interface: Vlan21 IP is disabled
hw_state[INGRESS] = not reduced, hw_state[EGRESS] = not reduced
mcast = 0
priority = 0
flags = 0x0
inbound label: 8
Feature IP_VACL:

FM_FEATURE_IP_VACL_INGRESS i/f: Vl21 map name: test

IP Seq. No: 10 Seq. Result : VACL_ACTION_FORWARD_CAPTURE
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMP Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - F-Mask Priority(H-High, L-Low)
Adj. = Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL = Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA = Sour.& Dest. Only VSAADA - Vlan SADA Only FF - Full Flow
VFF = Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error

<table>
<thead>
<tr>
<th>Indx</th>
<th>T</th>
<th>Dest Ip Addr</th>
<th>Source Ip Addr</th>
<th>DPort</th>
<th>SPort</th>
<th>Pro</th>
<th>RFM</th>
<th>X</th>
<th>ToS</th>
<th>MRTNP</th>
<th>Adj</th>
<th>FM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>V</td>
<td>22.2.2.2</td>
<td>21.1.1.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>V</td>
<td>32.2.2.2</td>
<td>31.1.1.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>V</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TM_PERMIT_RESULT

IP Seq. No: 65536 Seq. Result : VACL_ACTION_DROP

<table>
<thead>
<tr>
<th>Indx</th>
<th>T</th>
<th>Dest Ip Addr</th>
<th>Source Ip Addr</th>
<th>DPort</th>
<th>SPort</th>
<th>Pro</th>
<th>RFM</th>
<th>X</th>
<th>ToS</th>
<th>MRTNP</th>
<th>Adj</th>
<th>FM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>V</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TM_PERMIT_RESULT

Router>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show fm summary</td>
<td>Displays a summary of FM Information.</td>
</tr>
</tbody>
</table>
**show fm reflexive**

To display the information about the reflexive entry for the dynamic feature manager, use the `show fm reflexive` command in privileged EXEC mode.

```
show fm reflexive
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

This command has no default settings.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to display the information about the reflexive entry for the dynamic feature manager:

```
Router# show fm reflexive
Reflexive hash table:
    Vlan613:refacl, OUT-REF, 64060E0A, 64060D0A, 0, 0, 7, 783, 6
Router#
```

**show fm summary**

To display a summary of feature manager information, use the `show fm summary` command in user EXEC or privileged EXEC mode.

```
show fm summary
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

This command has no default settings.

### Command Modes

User EXEC Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Examples

This example shows how to display a summary of feature manager information:

Router>
```
show fm summary
Current global ACL merge algorithm:BDD
Interface:FastEthernet2/10
  ACL merge algorithm used:
    inbound direction: ODM
    outbound direction:BDD
  TCAM screening for features is ACTIVE outbound
  TCAM screening for features is ACTIVE inbound
Interface:FastEthernet2/26
  ACL merge algorithm used:
    inbound direction: ODM
    outbound direction:BDD
  TCAM screening for features is ACTIVE outbound
  TCAM screening for features is INACTIVE inbound
```
Router>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show fm interface</td>
<td>Displays the detailed information about the feature manager on a per-interface basis.</td>
</tr>
</tbody>
</table>

show funi

To display the frame-based user-network interface information, use the `show funi` command in user EXEC or privileged EXEC mode.

```
show funi {arp-server [atm atm-interface-number]|class-links
    [vpi/vci-value|value|value|value|connection-name]|ilmi-configuration|ilmi-status [atm atm-interface-number]|map|pvc{[vpi/vci-value|value|value|value|connection-name]|dbs|ppp]|route|traffic|vp atm-vpi-number|vc {atm-vcd-number|connection-name|detail [prefix 
    [interface|vc-name|vcd|vpi/vci]|]}|interface atm atm-interface-number|{connection-name|detail [prefix 
    [interface|vc-name|vcd|vpi/vci]|]}|range lower-vcd-limit upper-vcd-limit|connection-name|detail [prefix 
    [interface|vc-name|vcd|vpi/vci]|]}|interface atm atm-interface-number|{connection-name|detail [prefix 
    [interface|vc-name|vcd|vpi/vci]|]}|summary [atm atm-interface-number]}
```

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp-server</td>
<td>Displays Asynchronous Transfer Mode (ATM) address resolution protocol server table information.</td>
</tr>
<tr>
<td>atm atm-interface-number</td>
<td>(Optional) Specifies the ATM interface and the ATM interface number.</td>
</tr>
<tr>
<td>class-links</td>
<td>Displays ATM VC-class links information.</td>
</tr>
<tr>
<td>vpi/vci-value</td>
<td>(Optional) Specifies the Virtual Path Identifier or Virtual Channel Identifier (VPI/VCI) value (slash is mandatory).</td>
</tr>
<tr>
<td>vci-value</td>
<td>(Optional) Specifies the virtual circuit interface value.</td>
</tr>
<tr>
<td>connection-name</td>
<td>(Optional) Specifies the connection name.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ilmi-configuration</strong></td>
<td>Displays the top-level Integrated Local Management Interface (ILMI) information.</td>
</tr>
<tr>
<td><strong>ilmi-status</strong></td>
<td>Displays ATM interface ILMI information.</td>
</tr>
<tr>
<td><strong>map</strong></td>
<td>Displays ATM static mapping information.</td>
</tr>
<tr>
<td><strong>pvc</strong></td>
<td>Displays ATM Permanent Virtual Circuits (PVC) information.</td>
</tr>
<tr>
<td><strong>dbs</strong></td>
<td>Displays the DBS information on a virtual circuit.</td>
</tr>
<tr>
<td><strong>ppp</strong></td>
<td>Displays the PPP over ATM information</td>
</tr>
<tr>
<td><strong>route</strong></td>
<td>Displays ATM route information.</td>
</tr>
<tr>
<td><strong>traffic</strong></td>
<td>Displays ATM statistics.</td>
</tr>
<tr>
<td><strong>vp</strong></td>
<td>Displays ATM virtual path information.</td>
</tr>
<tr>
<td><strong>atm-vpi-number</strong></td>
<td>(Optional) Specifies the VPI number.</td>
</tr>
<tr>
<td><strong>vc</strong></td>
<td>Displays ATM virtual circuit information.</td>
</tr>
<tr>
<td><strong>atm-vcd-number</strong></td>
<td>(Optional) Specifies the ATM Virtual Circuit Descriptor (VCD) number.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>Displays the detailed information of all VCs.</td>
</tr>
<tr>
<td><strong>prefix</strong></td>
<td>(Optional) Specifies the prefix for the output ordering.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>Specifies the type of interface. When this keyword is used along with the prefix keyword it displays the interface values in ascending order.</td>
</tr>
<tr>
<td><strong>vc_name</strong></td>
<td>Displays the VC names in the alphabetical order.</td>
</tr>
<tr>
<td><strong>vcd</strong></td>
<td>Displays the VCD value in the ascending order.</td>
</tr>
<tr>
<td><strong>vpi/vci</strong></td>
<td>Displays the VPI/VCI value in the ascending order.</td>
</tr>
<tr>
<td><strong>range</strong></td>
<td>Displays the range of VCs.</td>
</tr>
<tr>
<td><strong>lower-vcd-limit</strong></td>
<td>Specifies the lower limit VCD value.</td>
</tr>
<tr>
<td><strong>upper-vcd-limit</strong></td>
<td>Specifies the upper limit VCD value.</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>Display summary of VCs.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 2.3</td>
<td>This command was implemented on Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use this command to display the frame-based user-network interface information with the available keywords and arguments.

Examples

The following is sample output from the `show funi traffic` command. The fields are self-explanatory:

```
Router# show funi traffic
Input OAM Queue: 0/4136 (size/max)
  0 Input packets
  0 Output packets
  0 Broadcast packets
  0 Packets received on non-existent VC
  0 Packets attempted to send on non-existent VC
  0 OAM cells received
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F5 InEndcc: 0, F5 InSegcc: 0,
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
  0 OAM cells sent
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 0 F5 OutRDI: 0
F5 OutEndcc: 0, F5 OutSegcc: 0,
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0 F4 OutAIS: 0
  0 OAM cell drops
```

The following is sample output from the `show funi vc detail prefix interface` command. The fields are self-explanatory:

```
Router# show funi vc detail prefix interface
Description: N/A
ATM2/0 ATM2/0: VCD: 1, VPI: 1, VCI: 100
    UBR, PeakRate: 0 (0 cps)
    AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCN: 0x0, Encapsize: 12
    OAM frequency: 0 second(s)
    Transmit priority 6
    InPkt: 0, OutPkt: 0, InByte: 0, OutByte: 0
    InCell: 0, OutCell: 0
    InProc: 0, OutProc: 0, Broadcasts: 0
    InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
    InPktDrop: 0, OutPktDrop: 0
    CrcErr: 0, SarTimeOut: 0, OverSizeSDUs: 0, LenViolation: 0, CPIE0
    Out CLP=1 Pkt: 0, Cells: 0
    OAM cells received: 0
    OAM cells sent: 0
    Status: INACTIVE
Description: N/A
ATM2/0 ATM2/0: VCD: 2, VPI: 1, VCI: 101
    UBR, PeakRate: 0 (0 cps)
    AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCN: 0x0, Encapsize: 12
    OAM frequency: 0 second(s)
    Transmit priority 6
```

The following is sample output from the `show funi vc detail prefix vc_name` command. The fields are self-explanatory:

```
Router# show funi vc detail prefix vc_name
Description: N/A
ATM2/0: VCD: 1, VPI: 1, VCI: 100
    UBR, PeakRate: 0 (0 cps)
    AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCN: 0x0, Encapsize: 12
    OAM frequency: 0 second(s)
    Transmit priority 6
```
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InCells: 0, OutCells: 0
InProc: 0, OutProc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0, Cells: 0
OAM cells received: 0
OAM cells sent: 0
Status: INACTIVE
Description: N/A
ATM2/0: VCD: 2, VPI: 1, VCI: 101
UBR, PeakRate: 0 (0 cps)
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0, Encapsize: 12
OAM frequency: 0 second(s)
InARP frequency: 15 minutes(s)
The following is sample output from the show funi vc detail prefix pvi/vci command. The fields are self-explanatory:

Router# show funi vc detail prefix vpi/vci
Description: N/A
VPI/VCI: 1/100 ATM2/0: VCD: 1, VPI: 1, VCI: 100
VPI/VCI: 1/100 UBR, PeakRate: 0 (0 cps)
VPI/VCI: 1/100 AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0, Encapsize: 2
VPI/VCI: 1/100 OAM frequency: 0 second(s)
VPI/VCI: 1/100 InARP frequency: 15 minutes(s)
VPI/VCI: 1/100 Transmit priority 6
VPI/VCI: 1/100 InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InCells: 0, OutCells: 0
VPI/VCI: 1/100 InProc: 0, OutProc: 0, Broadcasts: 0
VPI/VCI: 1/100 InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
VPI/VCI: 1/100 InPktDrops: 0, OutPktDrops: 0
VPI/VCI: 1/100 CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0
VPI/VCI: 1/100 Out CLP=1 Pkts: 0, Cells: 0
VPI/VCI: 1/100 OAM cells received: 0
VPI/VCI: 1/100 OAM cells sent: 0
VPI/VCI: 1/100 Status: INACTIVE
Description: N/A
VPI/VCI: 1/101 ATM2/0: VCD: 2, VPI: 1, VCI: 101
VPI/VCI: 1/101 UBR, PeakRate: 0 (0 cps)
VPI/VCI: 1/101 AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0, Encapsize: 2

**show identity policy**

To display identity policy information in a tabular form, use the `show identity policy` command in privileged EXEC mode.

```
show identity policy  [name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>(Optional) Name of the identity policy.</th>
</tr>
</thead>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SX</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Examples

The following is output from the `show identity policy` command:

```
Router# show identity policy
Policy Name  ACL       Redirect ACL   Redirect URL
-----------------------------------------------
p1            some-acl  NONE        NONE
p2            another-acl redirect-acl http://www.foo.com/bar.html
```

Router#

The following is output for the policy named p2:

```
Router# show identity policy p2
Name: p2
Description: NONE
Access-Group: another-acl
URL-Redirect Match ACL: redirect-acl
URL-Redirect URL: http://www.foo.com/bar.html
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-configuration</td>
<td>Displays the running configuration for a router.</td>
</tr>
</tbody>
</table>

show identity profile

To display identity profile information in a tabular form, use the `show identity profile` command in privileged EXEC mode.

```
show identity profile [{default|dot1x|eapoudp}]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>(Optional) Displays default identity profile information.</td>
</tr>
<tr>
<td>dot1x</td>
<td>(Optional) Displays 802.1x identity profile information.</td>
</tr>
<tr>
<td>eapoudp</td>
<td>(Optional) Displays EAPoUDP identity profile information.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SX</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following is output from the `show identity profile` command:

```
Router# show running identity profile
Service Type: default
Default Authorized Device Policy: NONE
Default Non-Authorized Device Policy: NONE
Device / Address / Mask Allowed Policy
```

Cisco IOS Configuration Fundamentals Command Reference

645
Cisco IP Phone Authorized DEFAULT
Service Type: dot1x
Default Authorized Device Policy: NONE
Default Non-Authorized Device Policy: NONE
Device / Address / Mask Allowed Policy

0001.0203.0405 / ffff.ffff.ffff Authorized p2
Service Type: eapoudp
Device / Address / Mask Allowed Policy

10.0.0.0 / 255.0.0.0 Authorized p1

Router#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-configuration</code></td>
<td>Displays the running configuration for a router.</td>
</tr>
</tbody>
</table>

### show install

To display information about installed packages, use the `show install` command in privileged EXEC mode.

```
show install {active |committed |inactive |log |package {bootflash: |flash: |webui:}|rollback |summary |uncommitted}
```

#### Syntax Description

- **active**: Displays information about active packages.
- **committed**: Displays package activations that are persistent.
- **inactive**: Displays inactive packages.
- **log**: Displays entries stored in the logging installation buffer.
- **package**: Displays metadata information about the package, including description, restart information, components in the package, and so on.
- **{bootflash: | flash: | harddisk: | webui:}**: Specifies the location of the install package.
- **rollback**: Displays the software set associated with a saved installation.
- **summary**: Displays information about the list of active, inactive, committed, and superseded packages.
- **uncommitted**: Displays package activations that are nonpersistent.

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use the show commands to view the status of the installed package.

Example

The following is sample output from the `show install package` command:

```
Device# show install package bootflash:isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Name: isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SS
Version: 16.5.1.0.199.1484082952..Everest
Platform: ISR4300
Package Type: dmp
Defect ID: CSCxxx
Package State: Added
Supersedes List: {}
Smu ID: 1
```

The following is sample output from the `show install summary` command:

```
Device# show install summary
Active Packages:
  bootflash:isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Inactive Packages:
  No packages
Committed Packages:
  bootflash:isr4300-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Uncommitted Packages:
  No packages
Device#
```

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

The following is sample output from the `show install log` command:

```
Device# show install log
[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add]: END SUCCESS Sun Feb 26 05:57:22 UTC 2017
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS Sun Feb 26 05:57:22 UTC 2017
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install</td>
<td>Installs SMU packages.</td>
</tr>
</tbody>
</table>
## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snapshot</strong></td>
<td>Requests snapshot actions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>slot</strong></th>
<th>Specifies the hardware slot. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>number</strong></td>
<td>The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you wanted to specify the SIP in SIP slot 2 of the router, enter 2 as the number.</td>
</tr>
<tr>
<td>• <strong>f0</strong></td>
<td>The ESP in ESP slot 0.</td>
</tr>
<tr>
<td>• <strong>f1</strong></td>
<td>The ESP in ESP slot 1.</td>
</tr>
<tr>
<td>• <strong>fp active</strong></td>
<td>The active ESP.</td>
</tr>
<tr>
<td>• <strong>fp standby</strong></td>
<td>The standby ESP.</td>
</tr>
<tr>
<td>• <strong>r0</strong></td>
<td>The RP in RP slot 0.</td>
</tr>
<tr>
<td>• <strong>r1</strong></td>
<td>The RP in RP slot 1.</td>
</tr>
<tr>
<td>• <strong>rp active</strong></td>
<td>The active RP.</td>
</tr>
<tr>
<td>• <strong>rp standby</strong></td>
<td>The standby RP.</td>
</tr>
</tbody>
</table>

| **status** | Displays the status of snapshot operations.                                 |

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC (#) Diagnostic Mode (diag)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use the **show platform software snapshot status** command to view the status of a bootflash snapshot request.

## Examples

This example shows how to view the status of bootflash snapshot requests on the processor in the RO slot.

```
router#show platform software snapshot R0 status
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request platform software snapshot</td>
<td>Use this command to display a snapshot of the bootflash.</td>
</tr>
</tbody>
</table>
show gsr through show monitor event trace

- show gsr through show monitor event trace, on page 650
show gsr through show monitor event trace

show gsr

To display hardware information on the Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show gsr** command in EXEC mode.

```
show gsr [chassis-info | details]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>chassis-info</strong></td>
</tr>
<tr>
<td>(Optional) Displays backplane NVRAM information.</td>
</tr>
<tr>
<td><strong>details</strong></td>
</tr>
<tr>
<td>(Optional) In addition to the information displayed, this option includes hexadecimal output of the backplane NVRAM information.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2GS</td>
<td>This command was introduced to support the Cisco 12000 series GSRs.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to determine the type of hardware installed in your Cisco 12000 series GSR router.

**Examples**

The following is sample output from the **show gsr** command for a Cisco 12012 router. This command shows the type and state of the card installed in the slot.

```
Router# show gsr
Slot 0  type = Route Processor
       state = IOS Running MASTER
Slot 7  type = 1 Port Packet Over SONET OC-12c/STM-4c
       state = Card Powered
Slot 16 type = Clock Scheduler Card
       state = Card Powered PRIMARY CLOCK
```

The following is sample output from the **show gsr chassis-info** command for a Cisco 12012 router:

```
Router# show gsr chassis-info
Backplane NVRAM [version 0x20] Contents -
   Chassis: type 12012 Fab Ver: 1
   Chassis S/N: ZQ24CS3WT86MGVHL
   PCA: 800-3015-1 rev: A0 dev: 257 HW ver: 1.0
   Backplane S/N: A109EXPR75FUNYJK
   MAC Addr: base 0000.EAB2.34FF block size: 1024
   RMA Number: 0x5F-0x2D-0x44 code: 0x01 hist: 0x1A
```
show gt64010 (7200)

To display all GT64010 internal registers and interrupt status on the Cisco 7200 series routers, use the `show gt64010` command in EXEC mode.

**show gt64010**

**Syntax Description**
This command has no arguments or keywords.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command displays information about the CPU interface, DRAM/device address space, device parameters, direct memory access (DMA) channels, timers and counters, and protocol control information (PCI) internal registers. The information is generally useful for diagnostic tasks performed by technical support only.

**Examples**
The following is a partial sample output for the `show gt64010` command:

```
Router# show gt64010
GT64010 Channel 0 DMA:
  dma_list=0x6088C3EC, dma_ring=0x4B018480, dma_entries=256
  dma_free=0x6088CECC, dma_reqt=0x6088CECC, dma_done=0x6088CECC
  thread=0x6088CEAC, thread_end=0x6088CEAC
  backup_thread=0x0, backup_thread_end=0x0
  dma_working=0, dma_complete=6231, post_coalesce_frames=6231
  exhausted_dma_entries=0, post_coalesce_callback=6231
GT64010 Register Dump: Registers at 0xB4000000
CPU Interface:
  cpu_interface_conf : 0x80030000 (b/s 0x00000380)
  addr_decode_err : 0xFFFFFFFF (b/s 0xFFFFFFFF)
Processor Address Space:
  ras10_low : 0x00000000 (b/s 0x00000000)
  ras10_high : 0x00000000 (b/s 0x00000000)
  ras10_high : 0x00000000 (b/s 0x00000000)
  ras10_high : 0x00000000 (b/s 0x00000000)
  ras32_low : 0x00000000 (b/s 0x00000000)
  ras32_high : 0x00000000 (b/s 0x00000000)
  cs20_low : 0x00000000 (b/s 0x00000000)
  cs20_high : 0x00000000 (b/s 0x00000000)
  cs3_boot_low : 0x00000000 (b/s 0x00000000)
  cs3_boot_high : 0x00000000 (b/s 0x00000000)
  pci_io_low : 0x00000000 (b/s 0x00000000)
  pci_io_high : 0x00000000 (b/s 0x00000000)
  pci_mem_low : 0x00000000 (b/s 0x00000000)
  pci_mem_high : 0x00000000 (b/s 0x00000000)
  internal_spc_decode : 0x00000000 (b/s 0x00000000)
  bus_err_low : 0x00000000 (b/s 0x00000000)
  bus_err_high : 0x00000000 (b/s 0x00000000)
```
show hardware

To display the hardware-specific information for a router, use the **show hardware** command in user EXEC or privileged EXEC mode.

**show hardware**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **show hardware** command to display the hardware specific information for a router.

**Examples**

The following is sample output from the **show hardware** command:

```
Router# show hardware
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(22)T,
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 10-Oct-08 10:10 by prod_rel_team
ROM: System Bootstrap, Version 12.2(4r)B2, RELEASE SOFTWARE (fc2)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(16), RELEASE SOFTWARE (fc4)
Router uptime is 1 day, 16 hours, 32 minutes
System returned to ROM by reload at 04:13:23 UTC Wed Aug 12 2009
System image file is "disk0:Default-IOS-Image-Do-Not-Delete"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/ww1/exportRYPTOTool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco 7206VXR (NPE400) processor (revision A) with 491520K/32768K bytes of memo.
Processor board ID 31410931
R7000 CPU at 350MHz, Implementation 39, Rev 3.3, 256KB L2 Cache
6 slot VXR midplane, Version 2.7
Last reset from power-on
PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb0_mb1 has a total of 600 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 180 bandwidth points
This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port Adaptor
Hardware Configuration Guidelines" on Cisco.com <http://www.cisco.com>
for c7200 bandwidth points oversubscription and usage guidelines.
```
2 FastEthernet interfaces
4 Serial interfaces
125K bytes of NVRAM.
62976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
125440K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2002

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays statistics for all interfaces configured on the router or access server.</td>
</tr>
</tbody>
</table>

show health-monitor

To display the system Health Monitor status information, use the show health-monitor command in user EXEC or privileged EXEC mode.

show health-monitor [summary]

Syntax Description

| summary | (Optional) Displays a summary of the status information. |

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display the state of the hardware and software subsystem. Health Monitor is a Cisco IOS subsystem that monitors the state of the individual hardware and software subsystems. This monitoring helps in early detection and recovery of faults in the subsystem.

Examples

The following is sample output from show health-monitor command. The fields are self explanatory.

Router# show health-monitor summary
Chassis:
  Power Supply       Failure
  Temperature        OK
  Fans               OK
Memory:
  Free Memory processor       OK
  Memory Fragmentation Processor OK
  Free Memory I/O            OK
  Memory Fragmentation I/O   OK
DFC's:
  Slot 1 - Empty DFC       Not in operation
  Slot 2 - Empty DFC       Not in operation
  Slot 3 - AS5X-FC         OK
  Slot 4 - Empty DFC       Not in operation
  Slot 5 - Empty DFC       Not in operation
  Slot 6 - Empty DFC       Not in operation
  Slot 7 - Empty DFC       Not in operation
**show history**

To list the commands you have entered in the current EXEC session, use the `show history` command in EXEC mode.

```
show  history
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command history feature provides a record of EXEC commands you have entered. The number of commands that the history buffer will record is determined by the `history size` line configuration command or the `terminal history size` EXEC command.

The table below lists the keys and functions you can use to recall commands from the command history buffer.

**Table 85: History Keys**

<table>
<thead>
<tr>
<th>Key</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or Up Arrow²</td>
<td>Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or Down Arrow¹</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
</tbody>
</table>

³ The arrow keys function only with ANSI-compatible terminals.

**Examples**

The following is sample output from the `show history` command, which lists the commands the user has entered in EXEC mode for this session:

```
Router# show history
   help
   where
   show hosts
   show history
Router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history size</td>
<td>Enables the command history function, or changes the command history buffer size for a particular line.</td>
</tr>
</tbody>
</table>
**Command**  

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal history size</td>
<td>Enables the command history feature for the current terminal session, or changes the size of the command history buffer for the current terminal session.</td>
</tr>
</tbody>
</table>

### show history all

To display command history and reload information of a router, use the `show history all` command in user EXEC or privileged EXEC mode.

`show history all`

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show history all` command to display command history and reload information of a router.

**Examples**

The following is sample output from the `show history all` command:

```
Router# show history all
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco 7206VXR (NPE400) processor (revision A) with 491520K/32768K bytes of memo.
Processor board ID 31410931
R7000 CPU at 350MHz, Implementation 39, Rev 3.3, 256KB L2, 4096KB L3 Cache
6 slot VXR midplane, Version 2.7
Last reset from power-on
PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb0_mb1 has a total of 600 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 180 bandwidth points
This configuration is within the PCI bus capacity and is supported.
Please refer to the following document “Cisco 7200 Series Port Adaptor Hardware Configuration Guidelines” on Cisco.com <http://www.cisco.com> for c7200 bandwidth points oversubscription and usage guidelines.
2 FastEthernet interfaces
4 Serial interfaces
125K bytes of NVRAM.
Installed image archive
```
Aug 12 04:17:08.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Nullp
Aug 12 04:17:08.419: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state p
Aug 12 04:17:08.419: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state p
Aug 12 04:17:08.419: %LINK-3-UPDOWN: Interface Serial2/0, changed state to down
Aug 12 04:17:08.419: %LINK-3-UPDOWN: Interface Serial2/1, changed state to down
Aug 12 04:17:08.419: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
Aug 12 04:17:08.419: %LINK-3-UPDOWN: Interface Serial3/1, changed state to up
Aug 12 04:17:08.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface SSLVPN-VIp
62976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
125440K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Aug 12 04:17:09.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherp
Aug 12 04:17:09.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherp
Aug 12 04:17:09.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0n
Aug 12 04:17:09.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1n
Aug 12 04:17:12.411: %LINK-3-UPDOWN: Interface Serial3/0, changed state to down
Aug 12 04:17:12.411: %LINK-3-UPDOWN: Interface Serial3/1, changed state to down
Aug 12 04:17:12.411: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0n
Aug 12 04:17:12.411: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1n
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]: yes
CMD: 'access-list 199 permit icmp host 10.10.10.10 host 20.20.20.20' 04:18:15 U9
CMD: 'crypto map NiStTeSt1 10 ipsec-manual' 04:18:15 UTC Wed Aug 12 2009
CMD: 'match address 199
' 04:18:15 UTC Wed Aug 12 2009
CMD: 'set peer 20.20.20.20
' 04:18:15 UTC Wed Aug 12 2009
CMD: 'exit' 04:18:15 UTC Wed Aug 12 2009
CMD: 'no access-list 199' 04:18:15 UTC Wed Aug 12 2009
CMD: 'no crypto map NiStTeSt1' 04:18:15 UTC Wed Aug 12 2009
Aug 12 04:18:15.403: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(22)T
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 10-Oct-08 10:10 by prod_rel_team
Aug 12 04:18:15.415: %ENTITY_ALARM-6-INFO: ASSERT INFO Fa0/0 Physical Port Adm
Aug 12 04:18:15.419: %ENTITY_ALARM-6-INFO: ASSERT INFO Fa0/1 Physical Port Adm
Aug 12 04:18:15.499: %CRYPTO-6-ISARMP_ON_OFF: ISARMP is OFF
Aug 12 04:18:15.599: %ENTITY_ALARM-6-INFO: ASSERT INFO Se2/0 Physical Port Adm
Aug 12 04:18:15.599: %ENTITY_ALARM-6-INFO: ASSERT INFO Se2/1 Physical Port Adm
Aug 12 04:18:15.599: %ENTITY_ALARM-6-INFO: ASSERT INFO Se3/0 Physical Port Adm
Aug 12 04:18:15.599: %ENTITY_ALARM-6-INFO: ASSERT INFO Se3/1 Physical Port Adm
Aug 12 04:18:15.599: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
Aug 12 04:18:15.823: %SYS-6-BOOTTIME: Time taken to reboot after reload = 314s
Aug 12 04:18:16.715: %LINK-5-CHANGED: Interface Serial2/0, changed state to ad
Aug 12 04:18:16.719: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to ad
Aug 12 04:18:16.723: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to ad
Aug 12 04:18:16.727: %LINK-5-CHANGED: Interface Serial2/1, changed state to adn
Aug 12 04:18:16.727: %LINK-5-CHANGED: Interface Serial3/0, changed state to adn
Aug 12 04:18:16.727: %LINK-5-CHANGED: Interface Serial3/1, changed state to adn
CMD: 'conf t' 04:18:30 UTC Wed Aug 12 2009
CMD: 'hostname 7206-3' 04:19:02 UTC Wed Aug 12 2009
CMD: 'ip host sjc-tftp02 171.69.17.17' 04:19:02 UTC Wed Aug 12 2009
CMD: 'ip host sjc-tftp01 171.69.17.19' 04:19:03 UTC Wed Aug 12 2009
CMD: 'ip host dirt 171.69.1.129' 04:19:03 UTC Wed Aug 12 2009
CMD: 'interface FastEther0/0' 04:19:03 UTC Wed Aug 12 2009
show gsr through show monitor event trace

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

```
show hosts [vrf vrf-name] [[view [[view-name|default]]] [all] [hostname|summary]]
```

**Syntax Description**

- **vrf vrf-name**  
  (Optional) The `vrf-name` argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view.

  **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

- **view view-name**  
  (Optional) The `view-name` argument specifies the DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) DNS view associated with the specified or global VRF.

  **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

- **default**  
  (Optional) Displays the default view.

- **all**  
  (Optional) Display all the host tables.

- **hostname**  
  (Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.

- **summary**  
  (Optional) The specified hostname cache information is to be displayed in brief summary format. Disables by default.
show hosts

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2T</td>
<td>Support was added for Cisco modem user interface feature.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>The vrf, all, and summary keywords and vrf-name and hostname arguments were added.</td>
</tr>
<tr>
<td>12.4(9)T</td>
<td>The view keyword and view-name argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

If you specify the show hosts command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q key to terminate command output.

Examples

The following is sample output from the show hosts command with no parameters specified:

```
Router# show hosts
Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the show hosts command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101
Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
Host     Port Flags Age Type Address(es)
user     None (perm, OK) 0 IP 192.0.2.001
www.example.com None (perm, OK) 0 IP 192.0.2.111 192.0.2.112
```
The table below describes the significant fields shown in the display.

**Table 86: show hosts Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default domain</td>
<td>Default domain name to be used to complete unqualified names if no domain list is defined.</td>
</tr>
<tr>
<td>Domain list</td>
<td>List of default domain names to be tried in turn to complete unqualified names.</td>
</tr>
<tr>
<td>Name/address lookup</td>
<td>Style of name lookup service.</td>
</tr>
<tr>
<td>Name servers</td>
<td>List of name server hosts.</td>
</tr>
<tr>
<td>Host</td>
<td>Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the <code>ip hosts</code> command.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.</td>
</tr>
<tr>
<td>Flags</td>
<td>Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• EX--Entries marked EX are expired.</td>
</tr>
<tr>
<td></td>
<td>• OK--Entries marked OK are believed to be valid.</td>
</tr>
<tr>
<td></td>
<td>• perm--A permanent entry is entered by a configuration command and is not timed out.</td>
</tr>
<tr>
<td></td>
<td>• temp--A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity.</td>
</tr>
<tr>
<td></td>
<td>• ??--Entries marked ?? are considered suspect and subject to revalidation.</td>
</tr>
<tr>
<td>Age</td>
<td>Number of hours since the software last referred to the cache entry.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of address. For example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the <code>ip hp-host global</code> configuration command, the <code>show hosts</code> command will display these hostnames as type HP-IP.</td>
</tr>
<tr>
<td>Address(es)</td>
<td>IP address of the host. One host may have up to eight addresses.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear host</code></td>
<td>Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.</td>
</tr>
<tr>
<td><code>ip host</code></td>
<td>Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.</td>
</tr>
</tbody>
</table>
show html

To display module and port information, use the `show html` command in privileged EXEC mode.

```
show html {module [ports [l2]]|port [{all|l2|l3}] [shortnames]} {command line|count|names|options}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module</td>
<td>Displays module information.</td>
</tr>
<tr>
<td>ports</td>
<td>(Optional) Displays the number of ports on the module.</td>
</tr>
<tr>
<td>l2</td>
<td>(Optional) Displays information about the Layer2 (l2) module.</td>
</tr>
<tr>
<td>port</td>
<td>Displays port information.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Displays information about the Layer 2 and Layer 3 modules.</td>
</tr>
<tr>
<td>l2</td>
<td>(Optional) Displays information about the Layer2 (l2) module.</td>
</tr>
<tr>
<td>l3</td>
<td>(Optional) Displays information about the Layer3 (l3) module.</td>
</tr>
<tr>
<td>shortnames</td>
<td>(Optional) Displays port short names.</td>
</tr>
<tr>
<td>command</td>
<td>Displays execute command over ports information.</td>
</tr>
<tr>
<td>line</td>
<td>Displays command to execute over modules information.</td>
</tr>
<tr>
<td>count</td>
<td>Displays the module count.</td>
</tr>
<tr>
<td>names</td>
<td>Displays the module names.</td>
</tr>
<tr>
<td>options</td>
<td>Displays the module options.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show html` command to display module and port information.

**Examples**

The following is sample output from the `show html` command using the `port` and `names` keywords. The field descriptions are self-explanatory.

```
Router# show html port names
this[0] = "FastEthernet0/0";
this[1] = "FastEthernet0/1";
this[2] = "Serial2/0";
this[3] = "Serial2/1";
this[4] = "Serial3/0";
```
The following is sample output from the **show html** command using the **port, all, and options** keywords. The output is self-explanatory.

```
Router# show html port all options
<option>FastEthernet0/0
<option>FastEthernet0/1
<option>Serial2/0
<option>Serial2/1
<option>Serial3/0
<option>Serial3/0.1
<option>Serial3/1
<option>Tunnel0
<option>Tunnel1
<option>Tunnel2
<option>Tunnel3
<option>Virtual-Access1
<option>Virtual-Template1
<option>VoIP-Null0
<option>vmi1
<option>vmi2
```

**show idb**

To display information about the status of interface descriptor blocks (IDBs), use the **show idb** command in privileged EXEC mode.

```
Router# show idb
```

**Syntax Description**

This command has nor arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>The output of this command was changed to show additional information.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **show idb** command:

```
Router# show idb
```
Maximum number of Software IDBs 8192. In use 17.

<table>
<thead>
<tr>
<th></th>
<th>HWIDBs</th>
<th>SWIDBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>5</td>
<td>14</td>
</tr>
<tr>
<td>Inactive</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Total IDBs</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>Size each (bytes)</td>
<td>5784</td>
<td>2576</td>
</tr>
<tr>
<td>Total bytes</td>
<td>86760</td>
<td>43792</td>
</tr>
</tbody>
</table>

HWIDB#1 1 2 GigabitEthernet0/0 0 5, HW IFINDEX, Ether)
HWIDB#2 2 3 GigabitEthernet9/0 0 5, HW IFINDEX, Ether)
HWIDB#3 3 4 GigabitEthernet9/1 6 5, HW IFINDEX, Ether)
HWIDB#4 4 5 GigabitEthernet9/2 6 5, HW IFINDEX, Ether)
HWIDB#5 13 1 Ethernet0 4 5, HW IFINDEX, Ether)

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In use</td>
<td>Total number of software IDBs (SWIDBs) that have been allocated. This number never decreases. SWIDBs are never deallocated.</td>
</tr>
<tr>
<td>Active</td>
<td>Total number of hardware IDBs (HWIDBs) and SWIDBs that are allocated and in use.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Total number of HWIDBs and SWIDBs that are allocated but not in use.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of HWIDBs and SWIDBs that are allocated.</td>
</tr>
</tbody>
</table>

**show idprom**

To display the identification programmable read-only memory (IDPROM) information for field-replaceable units (FRUs), use the `show idprom` command in privileged EXEC mode.

```
show idprom {all|frutype} [detail]
```

**Syntax Description**

- **all** Displays the information for all FRU types.
- **frutype** Type of FRU for information to be displayed; see the “Usage Guidelines” section for valid values.
- **detail** (Optional) Displays the detailed display of IDPROM data (verbose).

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SX</td>
<td>Support for this command on the Supervisor Engine 2 was integrated into Release 12.2(17d)SX.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>The module keyword was modified to support slot/subslot addressing for shared port adapters (SPAs) and SPA interface processors (SIPs), and the optional clei keyword was added. The interface keyword was replaced by the transceiver keyword.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

Valid entries for `frutype` are as follows:

- `backplane`
- `clock number` --1 and 2.
- `earl slot` -- See the following paragraph for valid slot values.
- `module slot | port | slot / subslot [clei]` -- See the following paragraphs for valid values and descriptions.
- `rp slot` -- See the following paragraph for valid slot values.
- `power-supply number` --1 and 2.
- `supervisor slot` -- See the following paragraph for valid slot values.
- `transceiver slot | subslot | port | slot | subslot GigabitEthernet | GigabitEthernetWAN]`
- `vtt number` --1 to 3.

The `module slot/port` argument designates the module slot location and port number.

Valid values for `slot` depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The `module {slot | slot/subslot [clei]}` syntax designates either the `slot` location alone of the SIP in the chassis (to show information for the SIP only), or the `slot` location of the SIP and the `subslot` location of a SPA installed within the SIP (to display information for a SPA only). Valid values for `slot` depend on the chassis model (2-13), and valid values for `subslot` depend on the SIP type (such as 0-3 for a Cisco 7600 SIP-200 and Cisco 7600 SIP-400). The optional `clei` keyword specifies display of the Common Language Equipment Identification (CLEI) information for the specified SIP or SPA.

Use the `show idprom backplane` command to display the chassis serial number.

Use the `transceiver slot / subslot / port` form of the command to display information for transceivers installed in a SPA, where `slot` designates the location of the SIP, `subslot` designates the location of the SPA, and `port` designates the interface number.

The `interface interface slot` keyword and arguments supported on GBIC security-enabled interfaces have been replaced by the `transceiver` keyword option.

To specify LAN Gigabit Ethernet interfaces, use the `show idprom transceiverslot/subslot GigabitEthernet` form of the command.

- To specify WAN Gigabit Ethernet interfaces, use the `show idprom transceiverslot/subslot GigabitEthernetWAN` form of the command.

### Examples

This example shows how to display IDPROM information for clock 1:
Router#

**show idprom clock 1**

IDPROM for clock #1

(FRU is 'Clock FRU')

OEM String = 'Cisco Systems'

Product Number = 'WS-C6000-CL'

Serial Number = 'SMT03073115'

Manufacturing Assembly Number = '73-3047-04'

Manufacturing Assembly Revision = 'A0'

Hardware Revision = 1.0

Current supplied (+) or consumed (-) = 0.000A

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

**Table 88: show idprom Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRU is</td>
<td>Indicates the type of the field-replacement unit (FRU) to which the information that follows applies.</td>
</tr>
<tr>
<td>OEM String</td>
<td>Names the original equipment manufacturer (OEM).</td>
</tr>
<tr>
<td>Product Number</td>
<td>A number that identifies a product line.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>A number that uniquely identifies the product itself.</td>
</tr>
<tr>
<td>Manufacturing Assembly Number</td>
<td>A number that identifies the hardware identification number.</td>
</tr>
<tr>
<td>Manufacturing Assembly Revision</td>
<td>A number that identifies the manufacturing assembly number.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>A number that represents the hardware upgrade.</td>
</tr>
<tr>
<td>Current supplied (+) or consumed (-)</td>
<td>Indicated the amount of electrical current that the device supplies or uses.</td>
</tr>
</tbody>
</table>

This example shows how to display IDPROM information for power supply 1:

Router#

**show idprom power-supply 1**

IDPROM for power-supply #1

(200V 220v AC power supply, 1360 watt)

OEM String = 'Cisco Systems, Inc.'

Product Number = 'WS-CAC-1300W'

Serial Number = 'ACP03020001'

Manufacturing Assembly Number = '34-0918-01'

Manufacturing Assembly Revision = 'A0'

Hardware Revision = 1.0

Current supplied (+) or consumed (-) = 27.460A

This example shows how to display detailed IDPROM information for power supply 1:

Router#

**show idprom power-supply 1 detail**

IDPROM for power-supply #1

IDPROM image:

(200V 220v AC power supply, 1360 watt)

IDPROM image block #0:
This example shows how to display IDPROM information for the backplane:

Router#  
show idprom backplane
IDPROM for backplane #0
(FRU is 'Catalyst 6000 9-slot backplane')
OEM String = 'Cisco Systems'
Product Number = 'WS-C6009'
Serial Number = 'SCA030900JA'
Manufacturing Assembly Number = '73-3046-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 1.0
Current supplied (+) or consumed (-) = 0.000A

The following example shows sample output for a Cisco 7600 SIP-400 installed in slot 3 of the router:

Router#  
show idprom module 3
IDPROM for module #3
(FRU is '4-subslot SPA Interface Processor-400')
OEM String = 'Cisco Systems'
Product Number = '7600-SIP-400'
Serial Number = 'JAB0851042X'
Manufacturing Assembly Number = '73-8404-10'
Manufacturing Assembly Revision = '09'
Hardware Revision = 0.95
Current supplied (+) or consumed (-) = -6.31A

The following example shows sample output for the clei form of the command on a Cisco 7600 SIP-200 installed in slot 2 of the router:

```
Router# show idprom module 2 clei
FRU    PID    VID    SN     CLEI
--------------- -------------------- --- ----------- ----------
module #2    7600-SIP-200    V01
```

The following example shows sample output for the detail form of the command on a Cisco 7600 SIP-400 installed in slot 3 of the router:

```
Router# show idprom module 3 detail
IDPROM for module #3
IDPROM image:
(FRU is '4-subslot SPA Interface Processor-400')
IDPROM image block #0:
block-signature = 0xABAB, block-version = 3,
block-length = 160, block-checksum = 4600
*** common-block ***
IDPROM capacity (bytes) = 512 IDPROM block-count = 2
FRU type = (0x6003,1103)
OEM String = 'Cisco Systems'
Product Number = '7600-SIP-400'
Serial Number = 'JAB085I042X'
Manufacturing Assembly Number = '73-8404-10'
Manufacturing Assembly Revision = '09'
Hardware Revision = 0.95
Manufacturing bits = 0x0 Engineering bits = 0x0
SNMP OID = 9.5.1.3.1.1.1.2.1103
Power Consumption = -631 centiamperes RMA failure code = 0-0-0-0
CLEI =
VID =
*** end of common block ***
IDPROM image block #1:
block-signature = 0x6003, block-version = 2,
block-length = 103, block-checksum = 2556
*** linecard specific block ***
feature-bits = 00000000 00000000
hardware-changes-bits = 00000000 00000000
card index = 158
mac base = 0012.4310.D840
mac_len = 128
num_processors = 1
epld_num = 0
epld_versions = 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
port numbers:
pair #0: type=00, count=00
pair #1: type=00, count=00
pair #2: type=00, count=00
pair #3: type=00, count=00
pair #4: type=00, count=00
pair #5: type=00, count=00
pair #6: type=00, count=00
pair #7: type=00, count=00
sram_size = 0
sensor_thresholds =
sensor #0: critical = 75 oC, warning = 60 oC
sensor #1: critical = 70 oC, warning = 55 oC
```
sensor #2: critical = 80 oC, warning = 65 oC
sensor #3: critical = 75 oC, warning = 60 oC
sensor #4: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #5: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #6: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #7: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)

max_connector_power = 3600
cooling_requirement = 35
ambient_temp = 55

*** end of linecard specific block ***

The following example shows sample output for a 4-Port OC-3c/STM-1 ATM SPA installed in subslot 0 of the SIP installed in slot 5 of the router:

Router# show idprom module 5/0
IDPROM for SPA module #5/0
(FRU is '4-port OC3/STM1 ATM Shared Port Adapter')
Product Identifier (PID) : SPA-4XOC3-ATM
Version Identifier (VID) : V01
PCB Serial Number : PRTA2604138
Top Assy. Part Number : 68-2177-01
73/68 Board Revision : 05
73/68 Board Revision : 01
Hardware Revision : 0.224
CLEI Code : UNASSIGNED

The following example shows sample output for the clei form of the command for a 4-Port OC-3c/STM-1 POS SPA installed in subslot 3 of the SIP installed in slot 2 of the router:

Router# show idprom module 2/3 clei
FRU PID VID SN CLEI
--------------- -------------------- --- ----------- ----------
SPA module #2/3 SPA-4XOC3-POS V01 PRTA0304155 UNASSIGNED

The following example shows sample output for the detail form of the command for a 4-Port OC-3c/STM-1 POS SPA installed in subslot 3 of the SIP installed in slot 2 of the router:

Router# show idprom module 2/3 detail
IDPROM for SPA module #2/3
(FRU is '4-port OC3/STM1 POS Shared Port Adapter')
EEPROM version : 4
Compatible Type : 0xFF
Controller Type : 1088
Hardware Revision : 0.230
Boot Timeout : 0 msecs
PCB Serial Number : PRTA0304155
Part Number : 73-9313-02
73/68 Board Revision : 04
Fab Version : 02
RMA Test History : 0
RMA Number : 0-0-0-0
RMA History : 0
Deviation Number : 0
Product Identifier (PID) : SPA-4XOC3-POS
Version Identifier (VID) : V01
Top Assy. Part Number : 68-2169-01
show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the `show inventory` command in user EXEC or privileged EXEC mode.

```
show inventory [raw] [entity]
```

**Syntax Description**

- **raw**: (Optional) Retrieves information about all of the Cisco products—referred to as entities—installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification.
- **entity**: (Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display very specific UDI information; for example “sfslot 1” will display the UDI information for slot 1 of an entity named sfslot.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(27)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(27)S.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(18)SXE5</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE5.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The `show inventory` command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the `show inventory` command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Examples

The following is sample output from the `show inventory` command without any keywords or arguments. This sample output displays a list of Cisco entities installed in a router that are assigned a PID.

```
Router# show inventory
NAME: "Chassis", DESCR: "12008/GRP chassis"
PID: GSR8/40 , VID: V01, SN: 63915640
NAME: "slot 0", DESCR: "GRP"
PID: GRP-B , VID: V01, SN: CAB021300R5
NAME: "slot 1", DESCR: "4 port ATM OC3 multimode"
PID: 4OC3/ATM-MM-SC , VID: V01, SN: CAB04036GT1
NAME: "slot 3", DESCR: "4 port OC3 POS multimode"
PID: LC-4OC3/POS-MM , VID: V01, SN: CAB014900GU
NAME: "slot 5", DESCR: "1 port Gigabit Ethernet"
PID: GE-GBIC-SC-B , VID: V01, SN: CAB034251NX
NAME: "slot 7", DESCR: "GRP"
PID: GRP-B , VID: V01, SN: CAB0428AN40
NAME: "slot 16", DESCR: "GSR 12008 Clock Scheduler Card"
PID: GSR8-CSC/ALRM , VID: V01, SN: CAB0429AUYH
NAME: "sfslot 1", DESCR: "GSR 12008 Switch Fabric Card"
PID: GSR8-SFC , VID: V01, SN: CAB0428ALOS
NAME: "sfslot 2", DESCR: "GSR 12008 Switch Fabric Card"
PID: GSR8-SFC , VID: V01, SN: CAB0429AU0M
NAME: "sfslot 3", DESCR: "GSR 12008 Switch Fabric Card"
PID: GSR8-SFC , VID: V01, SN: CAB0429ARD7
NAME: "PSslot 1", DESCR: "GSR 12008 AC Power Supply"
PID: FWR-GSR8-AC-B , VID: V01, SN: CAB041999CW
```

The table below describes the fields shown in the display.
For diagnostic purposes, the `show inventory` command can be used with the `raw` keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

The `raw` keyword option is primarily intended for troubleshooting problems with the `show inventory` command itself.

Router# show inventory raw
NAME: “Chassis”, DESCR: “12008/GRP chassis”
PID: , VID: V01, SN: 63915640
NAME: “slot 0”, DESCR: “GRP”
PID: , VID: V01, SN: CAB021300R5
NAME: “slot 1”, DESCR: “4 port ATM OC3 multimode”
PID: 4OC3/ATM-MM-SC , VID: V01, SN: CAB04036GT1
NAME: “slot 3”, DESCR: “4 port OC3 POS multimode”
PID: LC-4OC3/POS-MM , VID: V01, SN: CAB014900GU

Enter the `show inventory` command with an `entity` argument value to display the UDI information for a specific type of Cisco entity installed in the networking device. In this example, a list of Cisco entities that match the `sfslot` argument string is displayed.

Router# show inventory sfslot
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC , VID: V01, SN: CAB0428ALOS
NAME: “sfslot 2”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC , VID: V01, SN: CAB0429AU0M
NAME: “sfslot 3”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC , VID: V01, SN: CAB0429ARD7

You can request even more specific UDI information using the `show inventory` command with an `entity` argument value that is enclosed in quotation marks. In this example, only the details for the entity that exactly matches the `sfslot 1` argument string are displayed.

Router# show inventory “sfslot 1”
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC , VID: V01, SN: CAB0428ALOS
show location

To display the location information for an endpoint, use the `show location` command in user EXEC or privileged EXEC mode.

```
show location {{civic-location|custom-location|geo-location {identifier id|interface name type|static} }|host}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>civic-location</td>
<td>Specifies the civic location information.</td>
</tr>
<tr>
<td>custom-location</td>
<td>Specifies the custom location information.</td>
</tr>
<tr>
<td>geo-location</td>
<td>Specifies the geo-spatial location information.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the civic, custom, and geo-spatial host location information.</td>
</tr>
<tr>
<td>identifier id</td>
<td>Specifies the information identifier of the civic location, custom location, and geo-spatial location.</td>
</tr>
<tr>
<td>interface type number</td>
<td>Specifies the interface type and interface number.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies the configured location information.</td>
</tr>
</tbody>
</table>

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(40)SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(55)SE</td>
<td>This command was modified. The output was enhanced to display location information obtained from Cisco Discovery Protocol.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was modified. The <code>custom-location</code> and <code>geo-location</code> keywords were added.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

## Examples

The following sample output from the `show location civic-location` command displays all the civic location information for a specific identifier:

```
Device# show location civic-location identifier test
Civic location information
```
The following sample output from the `show location custom-location` command displays custom location information of a host device:

```
Device# show location custom-location identifier
Custom location information
---------------------------
Identifier: host
Name : bg115
Value : IDF2.5
```

The following sample output from the `show location geo-location` command displays geo-spatial location information of a device:

```
Device# show location geo-location identifier apjtpk
Geo location information
------------------------
Identifier : apjtpk
Latitude : 54.45
Longitude : 37.43
Altitude : 5 floor
Resolution : 54.45
```

The following sample output from the `show location host` command displays all host information of a device:

```
Device# show location host
Civic location information
--------------------------
Identifier : host
County : raps
City Division : SJ
Neighborhood : lake
Street Group : G2
Leading street direction: trav
Trailing street suffix : C76
Street number : 18
Street number suffix : 54
Landmark : KMD
Building : bg113
Unit : apjtpk
Floor : 3
Room : Andaman
Type of place : office
Postal community name : ios
Post office box : 12
Additional code : apjtpk
Seat : B5-10
Primary road name : outerringrd
Road section : east
Branch road name : venus
Sub branch road name : Tata
Street name postmodifier: ret
City : Boston
State : CA
Postal code : 1345
Additional location : cauveri
Custom location information
---------------------------
```
Identifier: host
Name: bg115
Value: IDF2.5

Geo location information
Identifier: host
Latitude: 12.34
Longitude: 56.78

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

Table 90: show location Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Information identifier of the civic location, custom location, and geo-spatial location.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the configured custom location identifier.</td>
</tr>
<tr>
<td>Value</td>
<td>Configured value of the custom location identifier.</td>
</tr>
<tr>
<td>Latitude</td>
<td>Configured latitude information of the device.</td>
</tr>
<tr>
<td>Longitude</td>
<td>Configured longitude information of the device.</td>
</tr>
<tr>
<td>Altitude</td>
<td>Configured altitude information of the device.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Configured resolution for the latitude and longitude.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location civic-location identifier</td>
<td>Configures the civic location information of a device.</td>
</tr>
<tr>
<td>location custom-location identifier</td>
<td>Configures the custom location information of a device.</td>
</tr>
<tr>
<td>location geo-location identifier</td>
<td>Configures the geo-spatial location of a device such as latitude, longitude, altitude, and resolution.</td>
</tr>
</tbody>
</table>

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the show logging command in privileged EXEC mode.

```
show logging [{slot slot-number|summary}]
```

Syntax Description

- **slot slot-number**: (Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 Internet router and from 0 to 7 for the Cisco 12008 Internet router.
- **summary**: (Optional) Displays counts of messages by type for each line card.

Command Modes

Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2 GS</td>
<td>The <strong>slot</strong> and <strong>summary</strong> keywords were added for the Cisco 12000.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>Command output was expanded to show the status of the logging count facility (“Count and time-stamp logging messages”).</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>Command output was expanded to show the status of XML syslog formatting.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>Command output was expanded (on supported software images) to show details about the status of system logging processed through the Embedded Syslog Manager (ESM). These lines appear as references to “filtering” or “filter modules”.</td>
</tr>
<tr>
<td>12.3(2)XE</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XE.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)SX.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>The CLI output was modified to show message discriminators defined at the router and syslog sessions associated with those message discriminators.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and which logging destinations (console, monitor, buffer, or host) logging is enabled. This command also displays Simple Network Management Protocol (SNMP) logging configuration parameters and protocol activity.

This command will display the contents of the standard system logging buffer, if logging to the buffer is enabled. Logging to the buffer is enabled or disabled using the `[no] logging buffered` command. The number of system error and debugging messages in the system logging buffer is determined by the configured size of the syslog buffer. This size of the syslog buffer is also set using the `logging buffered` command.

To enable and set the format for syslog message time stamping, use the `service timestamps log` command.

If debugging is enabled (using any `debug` command), and the logging buffer is configured to include level 7 (debugging) messages, debug output will be included in the system log. Debugging output is not formatted like system error messages and will not be preceded by the percent symbol (%).

Examples

The following is sample output from the `show logging` command on a software image that supports the Embedded Syslog Manager (ESM) feature:

```
Router# show logging
Syslog logging: enabled (10 messages dropped, 5 messages rate-limited,
  0 flushes, 0 overruns, xml disabled, filtering disabled)
  Console logging: level debugging, 31 messages logged, xml disabled,
  filtering disabled
  Monitor logging: disabled
  Buffer logging: level errors, 36 messages logged, xml disabled,
  filtering disabled
```
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled
No active filter modules.
Trap logging: level informational, 45 message lines logged

Log Buffer (8192 bytes):

The following example shows output from the `show logging` command after a message discriminator has been configured. Included in this example is the command to configure the message discriminator.

c7200-3(config)# logging discriminator ATTFLTR1 severity includes 1,2,5 rate-limit 100

Specified MD by the name ATTFLTR1 is not found.
Adding new MD instance with specified MD attribute values.
Router(config)# end

Router#
000036: *Oct 20 16:26:04.570: %SYS-5-CONFIG_I: Configured from console by console
Router# show logging

Syslog logging: enabled (11 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
Inactive Message Discriminator:
ATTFLTR1 severity group includes 1,2,5
    rate-limit not to exceed 100 messages per second
Console logging: level debugging, 25 messages logged, xml disabled, filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging: level debugging, 25 messages logged, xml disabled, filtering disabled
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled
No active filter modules.
Trap logging: level debugging, 28 message lines logged
Logging to 172.25.126.15 (udp port 1300, audit disabled, authentication disabled,
encryption disabled, link up),
28 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
Logging to 172.25.126.15 (tcp port 1307, audit disabled, authentication disabled,
encryption disabled, link up),
28 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled, filtering disabled
Logging to 172.20.1.1 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
28 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
Log Buffer (1000000 bytes):

The table below describes the significant fields shown in the output for the two preceding examples.
Table 91: show logging Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog logging:</td>
<td>Shows the general state of system logging (enabled or disabled), the status of logged messages (number of messages dropped, rate-limited, or flushed), and whether XML formatting or ESM filtering is enabled.</td>
</tr>
<tr>
<td>No Active Message</td>
<td>Indicates that a message discriminator is not being used.</td>
</tr>
<tr>
<td>Discriminator:</td>
<td></td>
</tr>
<tr>
<td>Inactive Message</td>
<td>Identifies a configured message discriminator that has not been invoked.</td>
</tr>
<tr>
<td>Discriminator:</td>
<td></td>
</tr>
<tr>
<td>Console logging:</td>
<td>Logging to the console port. Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled.</td>
</tr>
<tr>
<td></td>
<td>Corresponds to the configuration of the <code>logging console</code>, <code>logging console filtered</code>, or <code>logging console xml</code> command.</td>
</tr>
<tr>
<td>Monitor logging:</td>
<td>Logging to the monitor (all TTY lines). Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled.</td>
</tr>
<tr>
<td></td>
<td>Corresponds to the configuration of the <code>logging monitor</code>, <code>logging monitor filtered</code> or <code>logging monitor xml</code> command.</td>
</tr>
<tr>
<td>Buffer logging:</td>
<td>Logging to the standard syslog buffer. Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled.</td>
</tr>
<tr>
<td></td>
<td>Corresponds to the configuration of the <code>logging buffered</code>, <code>logging buffered filtered</code>, or <code>logging buffered xml</code> command.</td>
</tr>
<tr>
<td>Trap logging:</td>
<td>Logging to a remote host (syslog collector). Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled.</td>
</tr>
<tr>
<td></td>
<td>(The word “trap” means a trigger in the system software for sending error messages to a remote host.)</td>
</tr>
<tr>
<td></td>
<td>Corresponds to the configuration of the <code>logging host</code> command. The severity level limit is set using the <code>logging trap</code> command.</td>
</tr>
<tr>
<td>SNMP logging</td>
<td>Displays whether SNMP logging is enabled, the number of messages logged, and the retransmission interval. If not shown on your platform, use the <code>show logging history</code> command.</td>
</tr>
<tr>
<td>Logging Exception size</td>
<td></td>
</tr>
<tr>
<td>(8192 bytes)</td>
<td></td>
</tr>
<tr>
<td>Count and timestamp</td>
<td></td>
</tr>
<tr>
<td>logging messages:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Corresponds to the configuration of the <code>logging exception</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Corresponds to the configuration of the <code>logging count</code> command.</td>
</tr>
</tbody>
</table>
No active filter modules. Appears if no syslog filter modules are configured with the `logging filter` command.

Syslog filter modules are Tcl script files used when the Embedded Syslog Manager (ESM) is enabled. ESM is enabled when any of the `filtered` keywords are used in the logging commands.

If configured, the URL and filename of configured syslog filter modules will appear at this position in the output. Syslog filter modules are executed in the order in which they appear here.

Log Buffer (8192 bytes):
The value in parentheses corresponds to the configuration of the `logging buffered buffer-size` command. If no messages are currently in the buffer, the output ends with this line. If messages are stored in the syslog buffer, they appear after this line.

The following example shows that syslog messages from the system buffer are included, with time stamps. In this example, the software image does not support XML formatting or ESM filtering of syslog messages.

Router# `show logging`

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
  Console logging:disabled
  Monitor logging:level debugging, 0 messages logged
  Buffer logging:level debugging, 4104 messages logged
  Trap logging:level debugging, 4119 message lines logged
Logging to 192.168.111.14, 4119 message lines logged
Log Buffer (262144 bytes):
Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from 209.165.200.225 (afi 0) reaches 24, max 24
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
! NOTE THAT IT IS NOT PRECEEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxalew = 213866
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFXEXCEED:No. of prefix received from 209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor 209.165.200.226 3/1 (update malformed) 0 bytes
.
.

The software clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via Network Time Protocol (NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the “authoritative” flag is set, the flag prevents peers from synchronizing to the software clock.

The table below describes the symbols that precede the time stamp.
Table 92: Time-Stamping Symbols for Syslog Messages

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Time is not authoritative: the software clock is not in sync or has never been set.</td>
<td>*15:29:03.158 UTC Tue Feb 25 2003:</td>
</tr>
<tr>
<td>(blank)</td>
<td>Time is authoritative: the software clock is in sync or has just been set manually.</td>
<td>15:29:03.158 UTC Tue Feb 25 2003:</td>
</tr>
<tr>
<td>.</td>
<td>Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.</td>
<td>.15:29:03.158 UTC Tue Feb 25 2003:</td>
</tr>
</tbody>
</table>

The following is sample output from the `show logging summary` command for a Cisco 12012 router. A number in the column indicates that the syslog contains that many messages for the line card. For example, the line card in slot 9 has 1 error message, 4 warning messages, and 47 notification messages.

For similar log counting on other platforms, use the `show logging count` command.

The table below describes the logging level fields shown in the display.

Table 93: `show logging summary` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOT</td>
<td>Indicates the slot number of the line card. An asterisk next to the slot number indicates the GRP card whose error message counts are not displayed. For information on the GRP card, use the <code>show logging</code> command.</td>
</tr>
<tr>
<td>EMERG</td>
<td>Indicates that the system is unusable.</td>
</tr>
<tr>
<td>ALERT</td>
<td>Indicates that immediate action is needed.</td>
</tr>
<tr>
<td>CRIT</td>
<td>Indicates a critical condition.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging</td>
<td>Clears messages from the logging buffer.</td>
</tr>
<tr>
<td>logging buffered</td>
<td>Enables system message logging to a local buffer.</td>
</tr>
<tr>
<td>logging count</td>
<td>Enables the error log count capability.</td>
</tr>
<tr>
<td>logging history size</td>
<td>Changes the number of syslog messages stored in the history table of the router.</td>
</tr>
<tr>
<td>logging linecard</td>
<td>Logs messages to an internal buffer on a line card and limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.</td>
</tr>
<tr>
<td>service timestamps</td>
<td>Configures the system to time-stamp debugging or logging messages.</td>
</tr>
<tr>
<td>show logging count</td>
<td>Displays a summary of system error messages (syslog messages) by facility and severity.</td>
</tr>
<tr>
<td>show logging xml</td>
<td>Displays the state of system logging and the contents of the XML-specific logging buffer.</td>
</tr>
</tbody>
</table>

### show logging count

To display a summary of the number of times certain system error messages are occurring, use the `show logging count` command in privileged EXEC mode.

#### Syntax Description

This command has no arguements or keywords.

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

To enable the error log count capability (syslog counting feature), use the `logging count` command in global configuration mode.
This feature works independently of the various settings of the other logging commands (such as \texttt{no logging on}, \texttt{no logging buffered}, and so on). In other words, turning off logging by other means does not stop the counting and timestamping from occurring.

This command displays information such as the number of times a particular system error message occurs and the time stamp of the last occurrence of the specified message. System error messages are grouped into logical units called “Facilities” based on Cisco IOS software components.

To determine if system error message counting is enabled, use the \texttt{show logging} command.

The \texttt{service timestamps} command configuration determines the timestamp format (shown in the “Last Time” column) of \texttt{show logging count} command output. There is not quite enough space for all options of the possible options (datetime, milliseconds, and timezone) of the \texttt{service timestamps datetime} command to be displayed at the same time. As a result, if \texttt{msec} is selected, \texttt{timezone} will not be displayed. If \texttt{show-timezone} is selected but not \texttt{msec}, then the time zone will be displayed.

Occasionally, the length of the message name plus the facility name contains too many characters to be printed on one line. The CLI attempts to keep the name and facility name on one line but, if necessary, the line will be wrapped, so that the first line contains the facility name and the second line contains the message name and the rest of the columns.

### Examples

The following example shows the number of times syslog messages have occurred and the most recent time that each error message occurred. In this example, the \texttt{show logging} command is used to determine if the syslog counting feature is enabled:

```
Router# show logging | include count
Count and timestamp logging messages: enabled
Router# show logging count
Facility Message Name Sev Occur Last Time
------------------------------ ------------------------------- -----------------------------
SYS BOOTTIME              6  1 00:00:12
SYS RESTART               5  1 00:00:11
SYS CONFIG_I              5  1 00:00:05
------------------------------ ------------------------------- -----------------------------
SYS TOTAL 3
LINEPROTO UPDOWN          5 13 00:00:19
------------------------------ ------------------------------- -----------------------------
LINEPROTO TOTAL 13
LINK UPDOWN               3  1 00:00:18
LINK CHANGED              5 12 00:00:09
------------------------------ ------------------------------- -----------------------------
LINK TOTAL 13
SNMP COLDSTART            5  1 00:00:11
------------------------------ ------------------------------- -----------------------------
SNMP TOTAL 1
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility</td>
<td>The facility, such as syslog, from which these error messages are occurring.</td>
</tr>
<tr>
<td>Message Name</td>
<td>The name of this message.</td>
</tr>
</tbody>
</table>
### show logging count

This command displays information about the state of the system error message log count capability. The output includes the total number of error messages that have occurred for the specified facility.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sev</td>
<td>The severity level of this message.</td>
</tr>
<tr>
<td>Occur</td>
<td>How many times this message has occurred.</td>
</tr>
<tr>
<td>Last Time</td>
<td>The last (most recent) time this message occurred. Timestamping is by default based on the system uptime (for example “3w1d” indicates 3 weeks and 1 day from the last system reboot.)</td>
</tr>
<tr>
<td>Sys Total / Lineproto Total / Link Total / SNMP Total</td>
<td>Total number of error messages that have occurred for the specified Facility.</td>
</tr>
</tbody>
</table>

In the following example, the user is interested only in the totals:

```
Router# show logging count | include total
SYS TOTAL 3
LINEPROTO TOTAL 13
LINK TOTAL 13
SNMP TOTAL 1
```

### Related Commands

- **clear logging**: Clears messages from the logging buffer.
- **logging count**: Enables the system error message log count capability.
- **service timestamps**: Configures the system to time-stamp debugging or logging messages.
- **show logging**: Displays general information about the state of system logging.

### show logging history

To display information about the state of the syslog history table, use the `show logging history` command in privileged EXEC mode.

```
show logging history
```

### Syntax Description

This command has no arguments or keywords.

### Command Modes

- Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays information about the syslog history table, such as the table size, the status of messages, and text of messages stored in the table. Messages stored in the table are governed by the `logging history` global configuration command.
The following example shows sample output from the **show logging history** command. In this example, notifications of severity level 5 (notifications) through severity level 0 (emergencies) are configured to be written to the logging history table.

```
Router# show logging history
Syslog History Table: 1 maximum table entries, saving level notifications or higher
0 messages ignored, 0 dropped, 15 table entries flushed, SNMP notifications not enabled
  entry number 16: SYS-5-CONFIG_I
  Configured from console by console
  timestamp: 1110
Router#
```

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

**Table 95: show logging history Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum table entry</td>
<td>Number of messages that can be stored in the history table. Set with the <strong>logging history size</strong> command.</td>
</tr>
<tr>
<td>saving level notifications</td>
<td>Level of messages that are stored in the history table and sent to the SNMP server (if SNMP notification is enabled). The severity level can be configured with the <strong>logging history</strong> command.</td>
</tr>
<tr>
<td>messages ignored</td>
<td>Number of messages not stored in the history table because the severity level is greater than that specified with the <strong>logging history</strong> command.</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of messages that could not be processed due to lack of system resources. Dropped messages do not appear in the history table and are not sent to the SNMP server.</td>
</tr>
<tr>
<td>table entries flushed</td>
<td>Number of messages that have been removed from the history table to make room for newer messages.</td>
</tr>
<tr>
<td>SNMP notifications</td>
<td>Whether syslog traps of the appropriate level are sent to the SNMP server. The sending of syslog traps are enabled or disabled through the <strong>snmp-server enable traps syslog</strong> command.</td>
</tr>
<tr>
<td>entry number:</td>
<td>Number of the message entry in the history table. In the example above, the message “SYS-5-CONFIG_I Configured from console by console” indicates a syslog message consisting of the facility name (SYS), which indicates where the message came from, the severity level (5) of the message, the message name (CONFIG_I), and the message text.</td>
</tr>
<tr>
<td>timestamp</td>
<td>Time, based on the up time of the router, that the message was generated.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging</td>
<td>Clears messages from the logging buffer.</td>
</tr>
</tbody>
</table>
## show ip ports all

To display all the open ports on a device, use the `show ip ports all` command in user EXEC or privileged EXEC mode.

### Syntax Description

- **Command**: `show ip ports all`

  ```plaintext
  Syntax Description
  This command has no arguments or keywords.
  ```

### Command Default

- **Command Default**: No default behavior or values.

### Command Modes

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)EZ</td>
<td>This command was introduced on the Catalyst 3750-X and Catalyst 3560-X Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1</td>
<td>This command was implemented on Cisco ASR1000 Aggregation Series Routers, Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000V Series.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.

### Examples

The following is sample output from the `show ip ports all` command:

```plaintext
Device# show ip ports all

Proto  Local Address   Foreign Address   State   PID/Program Name
TCB    Local Address   Foreign Address   (state)
tcp    *:4786           *:*               LISTEN  221/[IOS]SMI IBC
server process
udp    *:2228          0.0.0.0:0         297/[IOS]L2TRACE
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging history</td>
<td>Limits syslog messages sent to the router's history table to a specified severity level.</td>
</tr>
<tr>
<td>logging history size</td>
<td>Changes the number of syslog messages that can be stored in the history table.</td>
</tr>
<tr>
<td>logging linecard</td>
<td>Logs messages to an internal buffer on a line card. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.</td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>The <code>[no] snmp-server enable traps syslog</code> form of this command controls (enables or disables) the sending of system-logging messages to a network management station.</td>
</tr>
</tbody>
</table>
show ip ports all

---

### TCP/UDP ports used by various Linux processes

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID/ Process name</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>127.0.0.1:7022</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>9519 sshd</td>
</tr>
<tr>
<td>udp</td>
<td>0.0.0.0:1812</td>
<td>0.0.0.0:*</td>
<td>25668</td>
<td>smd</td>
</tr>
<tr>
<td>udp</td>
<td>0.0.0.0:1813</td>
<td>0.0.0.0:*</td>
<td>25668</td>
<td>smd</td>
</tr>
<tr>
<td>udp6</td>
<td>:::1812</td>
<td>::::*</td>
<td>25668</td>
<td>smd</td>
</tr>
<tr>
<td>udp6</td>
<td>:::1813</td>
<td>::::*</td>
<td>25668</td>
<td>smd</td>
</tr>
<tr>
<td>tcp</td>
<td>127.0.0.1:7022</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>9519 sshd</td>
</tr>
</tbody>
</table>

After reconfiguring ip http server.

Device# show ip ports all

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID/Program Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCB</td>
<td>Local Address</td>
<td>Foreign Address</td>
<td>(state)</td>
<td></td>
</tr>
<tr>
<td>tcp</td>
<td>:::443</td>
<td>::::*</td>
<td>LISTEN</td>
<td>286/[IOS]HTTP</td>
</tr>
<tr>
<td>tcp</td>
<td>*:443</td>
<td><em>:</em></td>
<td>LISTEN</td>
<td>286/[IOS]HTTP</td>
</tr>
<tr>
<td>tcp</td>
<td>:::80</td>
<td>::::*</td>
<td>LISTEN</td>
<td>286/[IOS]HTTP</td>
</tr>
<tr>
<td>tcp</td>
<td>*:80</td>
<td><em>:</em></td>
<td>LISTEN</td>
<td>286/[IOS]HTTP</td>
</tr>
<tr>
<td>tcp</td>
<td>*:4786</td>
<td><em>:</em></td>
<td>LISTEN</td>
<td>221/[IOS]SMI IBC</td>
</tr>
<tr>
<td>udp</td>
<td>*:2228</td>
<td>0.0.0.0:0</td>
<td>297/[IOS]L2TRACE</td>
<td></td>
</tr>
</tbody>
</table>

The table below describes the significant fields shown in the display

### Table 96: Field Descriptions of show ip ports all

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Transport protocol used.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Device IP Address.</td>
</tr>
<tr>
<td>Foreign Address</td>
<td>Remote or peer address.</td>
</tr>
<tr>
<td>State</td>
<td>State of the connection. It can be listen, established or connected.</td>
</tr>
<tr>
<td>PID/Program Name</td>
<td>Process ID or name</td>
</tr>
</tbody>
</table>
show logging system

To display the System Event Archive (SEA) logs, use the `show logging system` command in user EXEC mode or privileged EXEC mode.

```
show logging system \[\{disk [file-location]last [num-of-last-log-msgs]\}\]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk</td>
<td>(Optional) Displays SEA log disk, where the logs will be stored.</td>
</tr>
<tr>
<td>disk file-location</td>
<td>(Optional) Displays SEA logs from the specified file location. The <code>disk</code> keyword when used along with <code>file-location</code> argument displays SEA logs from the specified file location.</td>
</tr>
<tr>
<td>num-of-last-log-msgs</td>
<td>(Optional) Displays the specified number of log messages.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SCC</td>
<td>This command was introduced for the Cisco uBR10012 Router in the Cisco IOS Software Release 12.2(33)SCC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show logging system` command displays the latest messages first.

**Examples**

The following example shows a sample output of the `show logging system` command that displays the specified number of latest system log messages:

```
Router# show logging system
-----------------------------------------------
1: 01/24/07 15:38:40 6/-1 : MAJ, GOLD, syndiagSyncPinnacle failed in slot 6
2: 01/24/07 15:38:40 6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1
3: 01/24/07 15:38:40 6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1
4: 01/24/07 15:38:40 6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1
5: 01/24/07 15:38:40 6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1
6: 01/24/07 15:38:40 6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1
```
The table below describes the significant fields shown in the display.

**Table 97: show logging system Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOD/SUB</td>
<td>Module or the submodule that generated the log message.</td>
</tr>
<tr>
<td>SEV</td>
<td>Severity level of the message.</td>
</tr>
<tr>
<td>COMP</td>
<td>Software component that has logged the message.</td>
</tr>
</tbody>
</table>

The following example shows a sample output of the show logging system command that displays SEA logs from the specified file location:

```
Router# show logging system disk disk0:my_log.dat
-----------------------------------------------------
1: 02/01/95 00:35:51 2/3/-1: MAJ, GOLD, lc_ctrl_proc_obfl_info:test SEA log in DFC:Diagnostic OBFL testing
2: 02/01/95 00:35:09 2/5/-1: MAJ, GOLD, diag_hit_sys_limit[3/2]: sp_netint_thr[0]
3: 02/01/95 00:35:09 2/5/-1: MAJ, GOLD, diag_hit_sys_limit[3/2]: SP[81%],Tx_rate[408], Rx_rate[0]
4: 02/01/95 00:35:08 2/5/-1: MAJ, GOLD, diag_hit_sys_limit[3/2]: sp_netint_thr[0]
5: 02/01/95 00:35:08 2/5/-1: MAJ, GOLD, diag_hit_sys_limit[3/2]: SP[82%],Tx_rate[453], Rx_rate[0]
6: 02/01/95 00:35:08 2/5/-1: MAJ, GOLD, test_c2cot_hm_ch0_test[3]: port 13, chnl 0,                Skipped Fabric Channel HM Test
7: 02/01/95 00:35:08 2/5/-1: MAJ, GOLD, fabric_hm_inband_loopback_test[3/13]:diag_hit_sys_limit!test skipped.
8: 02/01/95 00:35:08 2/5/-1: MAJ, GOLD, diag_hit_sys_limit[3/13]: sp_netint_thr[0]
9: 02/01/95 00:35:08 2/5/-1: MAJ, GOLD, diag_hit_sys_limit[3/13]: SP[83%],Tx_rate[453], Rx_rate[0]
```

Cisco uBR10012 Universal Broadband Router

The following example shows a sample output of the show logging system command on the Cisco uBR10012 Router:

```
Router# show logging system
-----------------------------------------------------
1: 05/06/09 04:10:11 6/0: NON, SEATEST, "Test disk1":"
```

The following command is used to identify the disk on PRE currently being used to store the sea_log.dat file. The following example shows a sample output of the show logging system disk command executed on the Cisco uBR10012 router:

```
Router# show logging system disk
SEA log disk: disk1:
The following command is used to view the specified number of log messages stored in the sea_log.dat file. The following example shows a sample output of the show logging system
```
last 10
command on the Cisco uBR10012 router:
Router# show logging system
last 10
=====================================================================
1: 05/06/09 04:47:48 5/0: NON, SEATEST, "Second Message"
2: 05/06/09 04:47:31 6/0: NON, SEATEST, "First Message"

Related Commands
<table>
<thead>
<tr>
<th>clear logging system</th>
<th>Clears the event records stored in the SEA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy logging system</td>
<td>Copies the archived system events to another location.</td>
</tr>
<tr>
<td>logging system</td>
<td>Enables or disables the SEA logging system.</td>
</tr>
</tbody>
</table>

show logging xml

To display the state of system message logging in an XML format, and to display the contents of the XML syslog buffer, use the show logging xml command in privileged EXEC mode.

show logging xml

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command displays the same syslog state information as the standard show logging command, but displays the information in XML format. This command also displays the content of the XML syslog buffer (if XML-formatted buffer logging is enabled).

Examples
The following example compares the output of the standard show logging command with the output of the show logging xml command so that you can see how the standard information is formatted in XML.

Router# show logging
Syslog logging: enabled (10 messages dropped, 6 messages rate-limited, 0 flushes, 0 overruns, xml enabled)
  Console logging: level debugging, 28 messages logged, xml enabled
  Monitor logging: level debugging, 0 messages logged, xml enabled
  Buffer logging: level debugging, 2 messages logged, xml enabled (2 messages logged)
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 35 message lines logged
  Logging to 10.2.3.4, 1 message lines logged, xml disabled
Logging to 192.168.2.1, 1 message lines logged, xml enabled

Log Buffer (8192 bytes):
00:04:20: %SYS-5-CONFIG_I: Configured from console by console
00:04:41: %SYS-5-CONFIG_I: Configured from console by console
Router: show logging xml
<syslog-logging status="enabled" msg-dropped="10" msg-rate-limited="6" flushes="0"
overruns="0"><xml>enabled</xml></syslog-logging>
<console-logging level="debugging"
messages-logged="28"><xml>enabled</xml></console-logging>
<monitor-logging level="debugging"
messages-logged="0"><xml>enabled</xml></monitor-logging>
<buffer-logging level="debugging" messages-logged="2"><xml>enabled</xml></buffer-logging>
<logging-exception size="8192 bytes"></logging-exception>
<count-and-timestamp-logging status="disabled"></count-and-timestamp-logging>
<trap-logging level="informational" messages-lines-logged="35"></trap-logging>
<logging-to><dest id="0" ipaddr="10.2.3.4" message-lines-logged="1">disabled</dest></logging-to>
<logging-to><dest id="1" ipaddr="192.168.2.1" message-lines-logged="1">enabled</dest></logging-to>
<log-xml-buffer size="44444 bytes"></log-xml-buffer>
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>00:04:20</time><args><arg
id="0">console</arg><arg id="1">console</arg></args></ios-log-msg>
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>00:04:41</time><args><arg
id="0">console</arg><arg id="1">console</arg></args></ios-log-msg>
Router:

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

**Table 98: show logging and show logging xml Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>XML Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog logging</td>
<td>The global state of system message logging (syslog); “enabled” or “disabled.”</td>
<td>syslog-logging</td>
</tr>
<tr>
<td>Console logging</td>
<td>State of logging to console connections.</td>
<td>console-logging</td>
</tr>
<tr>
<td>Monitor logging</td>
<td>State of logging to monitor (TTY and Telnet) connections.</td>
<td>monitor-logging</td>
</tr>
<tr>
<td>Buffer logging</td>
<td>State of logging to the local system logging buffer.</td>
<td>buffer-logging</td>
</tr>
<tr>
<td>Count and timestamp logging messages:</td>
<td>Indicates whether the logging count feature is enabled. Corresponds to the <strong>logging count</strong> command.</td>
<td>count-and-timestamp-logging</td>
</tr>
<tr>
<td>Trap logging</td>
<td>State of logging to a remote host.</td>
<td>trap-logging</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>Displays the contents of the standard syslog buffer.</td>
</tr>
<tr>
<td>show logging count</td>
<td>Displays counts of each system error message.</td>
</tr>
</tbody>
</table>
show memory

To display statistics about memory when Cisco IOS software, Cisco IOS XE or Software Modularity images are running, use the show memory command in user EXEC or privileged EXEC mode.

Cisco IOS software
show memory [memory-type] [free] [overflow] [summary] [poisoning]

Cisco IOS XE or Software Modularity
show memory

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory-type</td>
<td>(Optional) Memory type to display (processor, multibus, io, or sram). If memory-type is not specified, statistics for all memory types present are displayed.</td>
</tr>
<tr>
<td>free</td>
<td>(Optional) Displays free memory statistics.</td>
</tr>
<tr>
<td>overflow</td>
<td>(Optional) Displays details about memory block header corruption corrections when the exception memory ignore overflow global configuration command is configured.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.</td>
</tr>
<tr>
<td>poisoning</td>
<td>(Optional) Displays memory poisoning details, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Alloc PID</td>
</tr>
<tr>
<td></td>
<td>• Alloc Check</td>
</tr>
<tr>
<td></td>
<td>• Alloc PC</td>
</tr>
<tr>
<td></td>
<td>• Alloc Name</td>
</tr>
<tr>
<td></td>
<td>• Corrupt Ptr</td>
</tr>
<tr>
<td></td>
<td>• Corrupt Val</td>
</tr>
<tr>
<td></td>
<td>• TotalBytes</td>
</tr>
<tr>
<td></td>
<td>• MarkedBytes</td>
</tr>
<tr>
<td></td>
<td>• TIME</td>
</tr>
</tbody>
</table>

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
This command was enhanced with the **overflow** keyword to display details about memory block header corruption corrections.

The command output was updated to display information about transient memory pools.

The command output was updated to display information about transient memory pools.

This command was integrated into Cisco IOS Release 12.2(27)SBC.

This command was implemented in Cisco IOS Software Modularity images.

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

The **poisoning** keyword was added.

The **show memory** stand-alone command was introduced on the Cisco Catalyst 4500e Serfies Switches. The command functions as shown in the Cisco IOS XE or Software Modularity examples.

---

**Usage Guidelines**

**Cisco IOS Software**

The **show memory** command displays information about memory available after the system image decompresses and loads.

**Cisco IOS XE or Software Modularity**

Use the **show memory** command when a Cisco IOS XE or Software Modularity image is running to display a summary of system-wide memory utilization. To display details about POSIX and Cisco IOS style system memory information when Software Modularity images are running, use the **show memory detailed** command.

**Examples**

Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. To view the appropriate output, see the following sections:

- Cisco IOS Software
- Cisco IOS XE
- Cisco IOS Software Modularity

**Cisco IOS Software**

The following is sample output from the **show memory** command:

```
Router# show memory

Head Total (b) Used (b) Free (b) Lowest (b) Largest (b)
Processor B0EE38 5181896 2210036 2971860 2692456 2845368

Processor memory
Address Bytes Prev. Next Ref PrevF NextF Alloc FC What
B0EE38 1056 0 B0F280 1 18F132 List Elements
B0F280 2656 B0EE38 B0FD08 1 18F132 List Headers
```
The following is sample output from the `show memory free` command:

Router# **show memory free**

<table>
<thead>
<tr>
<th>Processor memory</th>
<th>Head</th>
<th>Total (b)</th>
<th>Used (b)</th>
<th>Free (b)</th>
<th>Lowest (b)</th>
<th>Largest (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>B0EE38</td>
<td>5181896</td>
<td>2210076</td>
<td>2971820</td>
<td>2692456</td>
<td>2845368</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>Prev.</th>
<th>Next</th>
<th>Ref</th>
<th>PrevF</th>
<th>NextF</th>
<th>Alloc</th>
<th>PC</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEB844</td>
<td>32</td>
<td>CEB7A4</td>
<td>CEB88C</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>96B894</td>
<td>SSE Manager</td>
<td></td>
</tr>
<tr>
<td>D35ED4</td>
<td>80</td>
<td>D35E30</td>
<td>D35F4C</td>
<td>0</td>
<td>0</td>
<td>D27AE8</td>
<td>96B894</td>
<td>SSE Manager</td>
<td></td>
</tr>
</tbody>
</table>

The output of the `show memory free` command contains the same types of information as the `show memory` output, except that only free memory is displayed, and the information is ordered by free list.

The first section of the display includes summary statistics about the activities of the system memory allocator. The table below describes the significant fields shown in the first section of the display.

**Table 99: show memory Field Descriptions--First Section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>Hexadecimal address of the head of the memory allocation chain.</td>
</tr>
<tr>
<td>Total(b)</td>
<td>Sum of used bytes plus free bytes.</td>
</tr>
<tr>
<td>Used(b)</td>
<td>Amount of memory in use.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of memory not in use.</td>
</tr>
<tr>
<td>Lowest(b)</td>
<td>Smallest amount of free memory since last boot.</td>
</tr>
<tr>
<td>Largest(b)</td>
<td>Size of largest available free block.</td>
</tr>
</tbody>
</table>

The second section of the display is a block-by-block listing of memory use. The table below describes the significant fields shown in the second section of the display.
Table 100: Characteristics of Each Block of Memory—Second Section

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of block (in bytes).</td>
</tr>
<tr>
<td>Prev.</td>
<td>Address of previous block (should match the address on previous line).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of next block (should match the address on next line).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of previous free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of next free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>What</td>
<td>Name of process that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>

The **show memory io** command displays the free I/O memory blocks. On the Cisco 4000 router, this command quickly shows how much unused I/O memory is available.

The following is sample output from the **show memory io** command:

```
Router# show memory io
Address  Bytes  Prev.  Next  Ref  PrevF  NextF  Alloc PC  What
6132DA0  59264  6132664  6141520  0  0  600DDEC  3FCF0  *Packet Buffer*
600DDEC  600DA4C  600FE68  0  6132DA0  600FE68  0
600FE68  600FAC8  600FE68  0  600DDEC  6011D54  0
6011D54  60119B4  6011FEO  0  600FE68  6013D54  0
614FCA0  832  614F564  614FEO  0  601FD54  6177640  0
6177640  2657056  6172E90  0  0  614FCA0  0  0
Total: 2723244
```

The following sample output displays details of a memory block overflow correction when the exception memory ignore overflow global configuration command is configured:

```
Router# show memory overflow
Count  Buffer Count  Last corrected  Crashinfo files
1  1  00:11:17  slot0:crashinfo_20030620-075755
Traceback  607D526C  608731A0  607172F8  607288E0  607A5688  607A566C
```

The report includes the amount of time since the last correction was made and the name of the file that logged the memory block overflow details.

The **show memory sram** command displays the free SRAM memory blocks. For the Cisco 4000 router, this command supports the high-speed static RAM memory pool to make it easier for you to debug or diagnose problems with allocation or freeing of such memory.

The following is sample output from the **show memory sram** command:

```
Router# show memory sram
Address  Bytes  Prev.  Next  Ref  PrevF  NextF  Alloc PC  What
```
The following sample output from the `show memory` command used on the Cisco 4000 router includes information about SRAM memory and I/O memory:

```
Router# show memory

<table>
<thead>
<tr>
<th>Head</th>
<th>Total (b)</th>
<th>Used (b)</th>
<th>Free (b)</th>
<th>Lowest (b)</th>
<th>Largest (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>49C724</td>
<td>28719324</td>
<td>1510864</td>
<td>27208460</td>
<td>26511644</td>
</tr>
<tr>
<td>I/O</td>
<td>6000000</td>
<td>4194304</td>
<td>1297088</td>
<td>2897216</td>
<td>2869248</td>
</tr>
<tr>
<td>SRAM</td>
<td>1000</td>
<td>65536</td>
<td>63400</td>
<td>2136</td>
<td>2136</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>Prev.</th>
<th>Next</th>
<th>Ref</th>
<th>PrevF</th>
<th>NextF</th>
<th>Alloc PC</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>2032</td>
<td>0</td>
<td>1F0</td>
<td>1</td>
<td>3E73E</td>
<td>Init*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17F0</td>
<td>2032</td>
<td>1000</td>
<td>1FE0</td>
<td>1</td>
<td>3E73E</td>
<td><em>Init</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1FE0</td>
<td>544</td>
<td>17F0</td>
<td>2200</td>
<td>1</td>
<td>3276A</td>
<td><em>Init</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2200</td>
<td>52</td>
<td>1FE0</td>
<td>2234</td>
<td>1</td>
<td>31D68</td>
<td><em>Init</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2234</td>
<td>52</td>
<td>2200</td>
<td>2268</td>
<td>1</td>
<td>31DA6</td>
<td><em>Init</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2268</td>
<td>52</td>
<td>2234</td>
<td>229C</td>
<td>1</td>
<td>31DF2</td>
<td><em>Init</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72F0</td>
<td>2032</td>
<td>6E5C</td>
<td>7AE0</td>
<td>1</td>
<td>3E73E</td>
<td>Init</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7AE0</td>
<td>38178</td>
<td>72F0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The `show memory summary` command displays a summary of all memory pools and memory usage per Alloc PC (address of the system call that allocated the block).

The following is a partial sample output from the `show memory summary` command. This output shows the size, blocks, and bytes allocated. Bytes equal the size multiplied by the blocks. For a description of the other fields, see the tables above.

```
Router# show memory summary

<table>
<thead>
<tr>
<th>Head</th>
<th>Total (b)</th>
<th>Used (b)</th>
<th>Free (b)</th>
<th>Lowest (b)</th>
<th>Largest (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>B0E30</td>
<td>5181896</td>
<td>2210216</td>
<td>2971680</td>
<td>2692456</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alloc PC</th>
<th>Size</th>
<th>Blocks</th>
<th>Bytes</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2AB2</td>
<td>192</td>
<td>1</td>
<td>192</td>
<td>IDB: Serial Info</td>
</tr>
<tr>
<td>0x70EC</td>
<td>92</td>
<td>2</td>
<td>184</td>
<td>Init</td>
</tr>
<tr>
<td>0xC916</td>
<td>128</td>
<td>50</td>
<td>6400</td>
<td>RIF Cache</td>
</tr>
<tr>
<td>0x76ADE</td>
<td>4500</td>
<td>1</td>
<td>4500</td>
<td>XDI data</td>
</tr>
<tr>
<td>0x76E84</td>
<td>4464</td>
<td>1</td>
<td>4464</td>
<td>XDI data</td>
</tr>
<tr>
<td>0x76EAC</td>
<td>692</td>
<td>1</td>
<td>692</td>
<td>XDI data</td>
</tr>
<tr>
<td>0x77764</td>
<td>408</td>
<td>1</td>
<td>408</td>
<td>Init</td>
</tr>
<tr>
<td>0x77776</td>
<td>116</td>
<td>1</td>
<td>116</td>
<td>Init</td>
</tr>
<tr>
<td>0x777A2</td>
<td>408</td>
<td>1</td>
<td>408</td>
<td>Init</td>
</tr>
<tr>
<td>0x777B2</td>
<td>116</td>
<td>1</td>
<td>116</td>
<td>Init</td>
</tr>
<tr>
<td>0xA4600</td>
<td>24</td>
<td>3</td>
<td>72</td>
<td>List</td>
</tr>
<tr>
<td>0xD9B5C</td>
<td>52</td>
<td>1</td>
<td>52</td>
<td>SSE Manager</td>
</tr>
</tbody>
</table>
```

Cisco IOS XE

The following is sample output from the `show memory` command when a Cisco IOS XE image is running.
Router# show memory
#show memory
System memory: 1943928K total, 735007K used, 1208921K free, 153224K kernel reserved
Lowest (b) : 641880064
Total (K)  Used (K)  Free (K)
Process  1141112  514129  626984
Config   802816    220879  581937

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

Table 101: show memory (Software Modularity Image) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>Total amount of memory on the device, in kilobytes.</td>
</tr>
<tr>
<td>used</td>
<td>Amount of memory in use, in kilobytes.</td>
</tr>
<tr>
<td>free</td>
<td>Amount of memory not in use, in kilobytes.</td>
</tr>
<tr>
<td>kernel reserved</td>
<td>Amount of memory reserved by the kernel, in kilobytes.</td>
</tr>
<tr>
<td>Process</td>
<td>Amount of memory used by processes.</td>
</tr>
<tr>
<td>Config</td>
<td>Amount of memory used by the configuration.</td>
</tr>
</tbody>
</table>

Cisco IOS Software Modularity

The following is sample output from the show memory command when a Cisco IOS Software Modularity image is running.

Router# show memory
System Memory: 262144K total, 116148K used, 145996K free 4000K kernel reserved

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

Table 102: show memory (Software Modularity Image) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>Total amount of memory on the device, in kilobytes.</td>
</tr>
<tr>
<td>used</td>
<td>Amount of memory in use, in kilobytes.</td>
</tr>
<tr>
<td>free</td>
<td>Amount of memory not in use, in kilobytes.</td>
</tr>
<tr>
<td>kernel reserved</td>
<td>Amount of memory reserved by the kernel, in kilobytes.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exception memory ignore overflow</td>
<td>Configures the Cisco IOS software to correct corruptions in memory block headers and allow a router to continue its normal operation.</td>
</tr>
</tbody>
</table>
show memory allocating-process

To display statistics on allocated memory with corresponding allocating processes, use the `show memory allocating-process` command in user EXEC or privileged EXEC mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>totals</td>
<td>(Optional) Displays allocating memory totals.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show memory allocating-process` command displays information about memory available after the system image decompresses and loads.

**Examples**

The following is sample output from the `show memory allocating-process` command:

```
Router# show memory allocating-process
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 44E03560 186632636 26131896 160500740 160402052 153078204
Fast 44DE3560 131072 58280 72764 72764 72764
Processor memory
Address Bytes Prev. Next Ref Alloc Proc Alloc PC What
6148EC40 1504 0 6148F24C 1 *Init* 602310FC List Elements
6148F24C 3004 6148EC40 6148FE34 1 *Init* 60231128 List Headers
6148FE34 9000 6148F24C 61492188 1 *Init* 6023C634 Interrupt Stack
61492188 44 6148FE34 614921E0 1 *Init* 60C17FD8 *Init*
614921E0 9000 61492188 61494534 1 *Init* 6023C634 Interrupt Stack
61494534 44 614921E0 6149458C 1 *Init* 60C17FD8 *Init*
6149458C 220 61494534 61494694 1 *Init* 602450F4 *Init*
61494694 4024 6149458C 61495678 1 *Init* 601CBD64 TTY data
```

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

**Table 103: show memory allocating-process Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>Hexadecimal address of the head of the memory allocation chain.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Total(b)</th>
<th>Sum of used bytes plus free bytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used(b)</td>
<td>Amount of memory in use in bytes.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of memory not in use (in bytes).</td>
</tr>
<tr>
<td>Lowest(b)</td>
<td>Smallest amount of free memory since last boot (in bytes).</td>
</tr>
<tr>
<td>Largest(b)</td>
<td>Size of largest available free block (in bytes).</td>
</tr>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev.</td>
<td>Address of the preceding block (should match the address on preceding row).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of the following block (should match the address on following row).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>What</td>
<td>Name of process that owns the block, or &quot;(fragment)&quot; if the block is a fragment, or &quot;(coalesced)&quot; if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show memory allocating-process totals` command:

```
Router# show memory allocating-process totals

<table>
<thead>
<tr>
<th>Processor</th>
<th>Head Total(b)</th>
<th>Used(b)</th>
<th>Free(b)</th>
<th>Lowest(b)</th>
<th>Largest(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast</td>
<td>44E03560</td>
<td>186632636</td>
<td>26142524</td>
<td>160490112</td>
<td>160402052</td>
</tr>
<tr>
<td></td>
<td>44DE3560</td>
<td>58280</td>
<td>72792</td>
<td>72792</td>
<td>72764</td>
</tr>
</tbody>
</table>

Allocator PC Summary for: Processor

<table>
<thead>
<tr>
<th>PC</th>
<th>Total</th>
<th>Count</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x4041AF8C</td>
<td>5710616</td>
<td>3189</td>
<td><em>Packet Data</em></td>
</tr>
<tr>
<td>0x4041AF9C</td>
<td>2845480</td>
<td>3190</td>
<td><em>Packet Header</em></td>
</tr>
<tr>
<td>0x404DBA2C</td>
<td>1694556</td>
<td>203</td>
<td>Process Stack</td>
</tr>
<tr>
<td>0x4046EAD8</td>
<td>1074080</td>
<td>56</td>
<td>Init</td>
</tr>
<tr>
<td>0x404B5F68</td>
<td>1049296</td>
<td>9</td>
<td>pak subblock chunk</td>
</tr>
<tr>
<td>0x41DCFC30</td>
<td>523924</td>
<td>47</td>
<td>TCL Chunks</td>
</tr>
<tr>
<td>0x404E2482</td>
<td>448920</td>
<td>6</td>
<td>Malloclite</td>
</tr>
<tr>
<td>0x4066E8AC</td>
<td>402304</td>
<td>56</td>
<td>Init</td>
</tr>
<tr>
<td>0x40033878</td>
<td>397108</td>
<td>1</td>
<td>Init</td>
</tr>
<tr>
<td>0x41273E24</td>
<td>320052</td>
<td>1</td>
<td>CEF: table event ring</td>
</tr>
<tr>
<td>0x404B510C</td>
<td>253152</td>
<td>24</td>
<td>TW Buckets</td>
</tr>
<tr>
<td>0x42248F3C</td>
<td>229428</td>
<td>1</td>
<td>Init</td>
</tr>
<tr>
<td>0x42248F2E</td>
<td>229428</td>
<td>1</td>
<td>Init</td>
</tr>
<tr>
<td>0x423FFC20</td>
<td>218048</td>
<td>5</td>
<td>Dn48oCIM</td>
</tr>
<tr>
<td>0x421CB530</td>
<td>208144</td>
<td>1</td>
<td>epa crypto blk</td>
</tr>
<tr>
<td>0x417A07F0</td>
<td>196764</td>
<td>3</td>
<td>L2TP Hash Table</td>
</tr>
<tr>
<td>0x403AFF50</td>
<td>187836</td>
<td>3</td>
<td>Init</td>
</tr>
</tbody>
</table>
```

The table below describes the significant fields shown in the display.
Table 104: show memory allocating-process totals Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>Hexadecimal address of the head of the memory allocation chain.</td>
</tr>
<tr>
<td>Total(b)</td>
<td>Sum of used bytes plus free bytes.</td>
</tr>
<tr>
<td>Used(b)</td>
<td>Amount of memory in use (in bytes).</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of memory not in use (in bytes).</td>
</tr>
<tr>
<td>Lowest(b)</td>
<td>Smallest amount of free memory since last boot (in bytes).</td>
</tr>
<tr>
<td>Largest(b)</td>
<td>Size of the largest available free block in bytes.</td>
</tr>
<tr>
<td>PC</td>
<td>Program counter</td>
</tr>
<tr>
<td>Total</td>
<td>Total memory allocated by the process (in bytes).</td>
</tr>
<tr>
<td>Count</td>
<td>Number of allocations.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the allocating process.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes memory</td>
<td>Displays memory used per process.</td>
</tr>
</tbody>
</table>

show memory dead

To display statistics on memory allocated by processes that have terminated, use the show memory dead command in user EXEC or privileged EXEC mode.

```
show memory dead [totals]
```

Syntax Description

<table>
<thead>
<tr>
<th>totals</th>
<th>(Optional) Displays memory totals for processes that have been terminated.</th>
</tr>
</thead>
</table>

Command Modes

User EXEC Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `show memory dead` command displays information about processes that have been terminated. Terminated processes accounts for memory allocated under another process.
The following is sample output from the `show memory dead` command:

```
Router# show memory dead
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
I/O 600000 2097152 461024 1636128 1635224 1635960
```

### Processor memory

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>Prev.</th>
<th>Next</th>
<th>Ref</th>
<th>PrevF</th>
<th>NextF</th>
<th>Alloc PC</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>1D8310</td>
<td>60</td>
<td>1D82C8</td>
<td>1D8378</td>
<td>1</td>
<td></td>
<td></td>
<td>3281FFE</td>
<td>Router Init</td>
</tr>
<tr>
<td>2CA964</td>
<td>36</td>
<td>2CA914</td>
<td>2CA9B4</td>
<td>1</td>
<td></td>
<td></td>
<td>3281FFE</td>
<td>Router Init</td>
</tr>
<tr>
<td>2CAA04</td>
<td>112</td>
<td>2CA9B4</td>
<td>2CAA0</td>
<td>1</td>
<td></td>
<td></td>
<td>3A42144</td>
<td>OSPF Stub LSA RBTree</td>
</tr>
<tr>
<td>2CAA0</td>
<td>68</td>
<td>2CAA0</td>
<td>2CAB10</td>
<td>1</td>
<td></td>
<td></td>
<td>3A420D4</td>
<td>Router Init</td>
</tr>
<tr>
<td>2ED714</td>
<td>52</td>
<td>2ED668</td>
<td>2ED774</td>
<td>1</td>
<td></td>
<td></td>
<td>3381C84</td>
<td>Router Init</td>
</tr>
<tr>
<td>2F12AC</td>
<td>44</td>
<td>2F124C</td>
<td>2F1304</td>
<td>1</td>
<td></td>
<td></td>
<td>3A50234</td>
<td>Router Init</td>
</tr>
<tr>
<td>2F1304</td>
<td>24</td>
<td>2F12AC</td>
<td>2F1348</td>
<td>1</td>
<td></td>
<td></td>
<td>3A420D4</td>
<td>Router Init</td>
</tr>
<tr>
<td>2F1348</td>
<td>68</td>
<td>2F1304</td>
<td>2F13B8</td>
<td>1</td>
<td></td>
<td></td>
<td>3381C84</td>
<td>Router Init</td>
</tr>
<tr>
<td>300C28</td>
<td>340</td>
<td>300A14</td>
<td>300DA8</td>
<td>1</td>
<td></td>
<td></td>
<td>3381B42</td>
<td>Router Init</td>
</tr>
</tbody>
</table>

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

### Table 105: `show memory dead` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>Hexadecimal address of the head of the memory allocation chain.</td>
</tr>
<tr>
<td>Total(b)</td>
<td>Sum of used bytes plus free bytes.</td>
</tr>
<tr>
<td>Used(b)</td>
<td>Amount of memory in use.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of memory not in use (in bytes).</td>
</tr>
<tr>
<td>Lowest(b)</td>
<td>Smallest amount of free memory since last boot (in bytes).</td>
</tr>
<tr>
<td>Largest(b)</td>
<td>Size of the largest available free block (in bytes).</td>
</tr>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block (in bytes).</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev.</td>
<td>Address of the preceding block.</td>
</tr>
<tr>
<td>Next</td>
<td>Address of the following block.</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of the preceding free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of the following free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>
**show memory debug incremental**

To display information about memory leaks after a starting time has been established, use the `show memory debug incremental` command in privileged EXEC mode.

```
show memory debug incremental {allocations|leaks{[lowmem|summary]|status}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allocations</td>
<td>Displays all memory blocks that were allocated after issuing the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td>leaks</td>
<td>Displays only memory that was leaked after issuing the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td>lowmem</td>
<td>(Optional) Forces the memory leak detector to work in low memory mode, making no memory allocations.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Reports summarized memory leaks based on allocator_pc and size of the memory block.</td>
</tr>
<tr>
<td>status</td>
<td>Displays all memory blocks that were allocated after issuing the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4T</td>
<td>The summary keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show memory debug incremental allocations` command displays all the memory blocks that were allocated after the `set memory debug incremental starting-time` command was entered. The displayed memory blocks are just memory allocations, they are not necessarily leaks.

The `show memory debug incremental leaks` command provides output similar to the `show memory debug leaks` command, except that it displays only memory that was leaked after the `set memory debug incremental starting-time` command was entered.

The `show memory debug incremental leaks lowmem` command forces memory leak detection to work in low memory mode. The amount of time taken for analysis is considerably greater than that of normal mode. The output for this command is similar to the `show memory debug leaks` command, except that it displays only memory that was leaked after the `set memory debug incremental starting-time` command was entered. You can use this command when you already know that normal mode memory leak detection will fail (perhaps by an unsuccessful previous attempt to invoke normal mode memory leak detection).

The `show memory debug incremental leaks summary` command displays a summarized report of the memory that was leaked after the `set memory debug incremental starting-time` command was entered, ordered by allocator process call address (Alloc_pc) and by memory block size.

The `show memory debug incremental status` command displays whether a starting point for incremental analysis has been set and the elapsed time since then.
All show memory debug commands must be used on customer networks only to diagnose the router for memory leaks when memory depletion is observed. These CLI’s will have high CPU utilization and might result in time sensitive protocols to flap. These CLI’s are recommended for customer use, only in the maintenance window when the router is not in a scaled condition.

Note

All memory leak detection commands invoke normal mode memory leak detection, except when the low memory option is specifically invoked by use of the \texttt{lowmem} keyword. In normal mode, if memory leak detection determines that there is insufficient memory to proceed in normal mode, it will display an appropriate message and switch to low memory mode.

\textbf{Examples}

\texttt{show memory debug incremental allocations Command Example}

The following example shows output from the \texttt{show memory debug incremental} command when entered with the \texttt{allocations} keyword:

```
Router# show memory debug incremental allocations
Address Size Alloc_pc PID Name
62DA4E98 176 608C7C 44 CDP Protocol
62DA4F48 88 608C88 44 CDP Protocol
62DA4FA0 88 606224A 3 Exec
62DA4FF8 96 606224A 3 Exec
635B0F40 96 606224A 3 Exec
63905B50 200 606A4DA4 69 Process Events
```

\texttt{show memory debug incremental leaks summary Command Example}

The following example shows output from the \texttt{show memory debug incremental} command when entered with the \texttt{leaks} and \texttt{summary} keywords:

```
Router# show memory debug incremental leaks summary
Adding blocks for GD...
PCI memory
Alloc PC Size Blocks Bytes What
0x60874198 000000052 000000052 Exec
0x60874198 000000060 000000060 Exec
0x60874198 000000100 000000100 Exec
0x60874228 0000000052 0000000052 Exec
0x60874228 0000000060 0000000060 Exec
0x60874228 0000000100 0000000100 Exec
```

Cisco IOS Configuration Fundamentals Command Reference
show memory debug incremental status Command Example

The following example shows output from the show memory debug incremental command entered with the status keyword:

```
Router# show memory debug incremental status
Incremental debugging is enabled
Time elapsed since start of incremental debugging: 00:00:10
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set memory debug incremental starting-time</td>
<td>Sets the current time as the starting time for incremental analysis.</td>
</tr>
<tr>
<td>show memory debug leaks</td>
<td>Displays detected memory leaks.</td>
</tr>
</tbody>
</table>

show memory debug leaks

To display detected memory leaks, use the show memory debug leaks command in privileged EXEC mode. This command does not have a no form.

Cisco IOS software
```
show memory debug leaks [{chunks|largest|lowmem|summary}]
```

Cisco Catalyst 4500e Series Switches running IOS XE software
```
show memory debug leaks all [{detailed|totals}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays the information about leak block of the internal memory.</td>
</tr>
<tr>
<td>detailed (Optional)</td>
<td>Displays the detailed information about memory debug leak.</td>
</tr>
<tr>
<td>chunks (Optional)</td>
<td>Displays the memory leaks in chunks.</td>
</tr>
<tr>
<td>largest (Optional)</td>
<td>Displays the top ten leaking allocator_pcs based on size, and the total amount of memory they have leaked.</td>
</tr>
<tr>
<td>lowmem (Optional)</td>
<td>Forces the memory leak detector to work in low memory mode, making no memory allocations.</td>
</tr>
<tr>
<td>summary (Optional)</td>
<td>Reports summarized memory leaks based on allocator_pc and size of the memory block.</td>
</tr>
<tr>
<td>totals (Optional)</td>
<td>Displays summary report with the total number of each process.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 12.3(8)T1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

If optional keywords are not specified, the **show memory debug leaks** command invokes normal mode memory leak detection and does not look for memory leaks in chunks.

The **show memory debug leaks chunks** command invokes normal mode memory leak detection and looks for leaks in chunks as well.

The **show memory debug leaks largest** command displays the top ten leaking allocator_pcs and the total amount of memory that they have leaked. Additionally, each time when this command is invoked, it remembers the report of the previous invocation and compares it with the report of the current invocation. If there are new entries in the current report, they are tagged as “inconclusive.” If the same entry appears in the report of the previous invocation and the report of the current invocation, the inconclusive tag is not added. It is beneficial to run memory leak detection more than once and to consider only the consistently reported leaks.

The **show memory debug leaks lowmem** command forces memory leak detection to work in low memory mode. The amount of time taken for analysis is considerably greater than that of normal mode. The output for this command is similar to the **show memory debug leaks** command. You can use this command when you know that the normal mode memory leak detection fails (perhaps by an unsuccessful previous attempt to invoke normal mode memory leak detection).

The **show memory debug leaks summary** command reports memory leaks based on allocator_pc and then on the size of the block.

The **show memory debug leaks all detailed** command provides the details of memory leaks for a particular process.

The **show memory debug leaks all totals** command provides the summary report with the total number of memory leaks of each running process.

---

**Note**

All **show memory debug** commands must be used on customer networks only to diagnose the router for memory leaks when memory depletion is observed. These CLIs have high CPU utilization and might result in time sensitive protocols to flap. These CLIs are recommended for customer use, only in the maintenance window when the router is not in a scaled condition.

**Note**

The command **show memory debug leak lowmem** is extremely CPU intensive and can result in CPUHOG/WATCHDOG crash. This command must be used only when the router has reached an unusable state due to memory exhaustion. Its use on high end platforms such as ISR and above can potentially crash the box. Use of this command outside of these limitations can cause a console hang of one hour in some cases. As an alternative, use the **show memory debug leak** command.
Cisco IOS Software

**show memory debug leaks Command Example**

The following example shows output from the `show memory debug leaks` command:

```
Device# show memory debug leaks
Adding blocks for GD...
PCI memory
<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
<th>Alloc_pc</th>
<th>PID</th>
<th>Name</th>
</tr>
</thead>
</table>
| I/O memory
| Address | Size  | Alloc_pc | PID | Name |
| Processor memory
| Address | Size  | Alloc_pc | PID | Name |

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

**Table 106: show memory debug leaks Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the leaked block.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the leaked block (in bytes).</td>
</tr>
<tr>
<td>Alloc_pc</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>PID</td>
<td>The process identifier of the process that allocated the block.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the process that allocated the block.</td>
</tr>
</tbody>
</table>
```

**show memory debug leaks chunks Command Example**

The following example shows output from the `show memory debug leaks chunks` command:

```
Router# show memory debug leaks chunks
Adding blocks for GD...
PCI memory
| Address | Size  | Alloc_pc | PID | Name |
| Chunk Elements:
| Address | Size  | Parent | Name |
| I/O memory
| Address | Size  | Alloc_pc | PID | Name |
```
Chunk Elements:
<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
<th>Parent</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>62DABD28</td>
<td>80</td>
<td>60616750</td>
<td>-2 Init</td>
</tr>
<tr>
<td>62DABD78</td>
<td>80</td>
<td>606167A0</td>
<td>-2 Init</td>
</tr>
<tr>
<td>62DCF240</td>
<td>88</td>
<td>605B7E70</td>
<td>-2 Init</td>
</tr>
<tr>
<td>62DCF298</td>
<td>96</td>
<td>605B7E98</td>
<td>-2 Init</td>
</tr>
<tr>
<td>62DCF2F8</td>
<td>88</td>
<td>605B7EB4</td>
<td>-2 Init</td>
</tr>
<tr>
<td>62DCF350</td>
<td>96</td>
<td>605B7EDC</td>
<td>-2 Init</td>
</tr>
<tr>
<td>63336C28</td>
<td>104</td>
<td>60C67D74</td>
<td>-2 Init</td>
</tr>
<tr>
<td>63370D58</td>
<td>96</td>
<td>60C656AC</td>
<td>-2 Init</td>
</tr>
<tr>
<td>633710A0</td>
<td>304</td>
<td>60C656AC</td>
<td>-2 Init</td>
</tr>
<tr>
<td>63B2BF68</td>
<td>96</td>
<td>60C659D4</td>
<td>-2 Init</td>
</tr>
<tr>
<td>63BA3FE0</td>
<td>32832</td>
<td>608D2848</td>
<td>104 Audit Process</td>
</tr>
<tr>
<td>63BB4020</td>
<td>32832</td>
<td>608D2FD8</td>
<td>104 Audit Process</td>
</tr>
</tbody>
</table>

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

### show memory debug leaks chunks command

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

#### Table 107: show memory debug leaks chunks Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the leaked block.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the leaked block (in bytes).</td>
</tr>
<tr>
<td>Alloc_pc</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>PID</td>
<td>The process identifier of the process that allocated the block.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the process that allocated the block.</td>
</tr>
<tr>
<td>Size</td>
<td>(Chunk Elements) Size of the leaked element (bytes).</td>
</tr>
<tr>
<td>Parent</td>
<td>(Chunk Elements) Parent chunk of the leaked chunk.</td>
</tr>
<tr>
<td>Name</td>
<td>(Chunk Elements) The name of the leaked chunk.</td>
</tr>
</tbody>
</table>

**show memory debug leaks largest Command Example**

The following example shows output from the `show memory debug leaks largest` command:

```
Router# show memory debug leaks largest
```
Adding blocks for GD...

- **PCI memory**
  - Alloc_pc total leak size
  - I/O memory
  - Alloc_pc total leak size
  - Processor memory

Alloc_pc total leak size
608D2848 32776 inconclusive
608D2FD8 32776 inconclusive
60C656AC 288 inconclusive
60C67D74 48 inconclusive
605B7E98 40 inconclusive
605B7EDC 40 inconclusive
60C659D4 40 inconclusive
605B7E70 32 inconclusive
605B7EB4 32 inconclusive
60616750 24 inconclusive

The following example shows output from the second invocation of the `show memory debug leaks largest` command:

```
Router# show memory debug leaks largest
Adding blocks for GD...
- **PCI memory**
  - Alloc_pc total leak size
  - I/O memory
  - Alloc_pc total leak size
  - Processor memory

Alloc_pc total leak size
608D2848 32776
608D2FD8 32776
60C656AC 288
60C67D74 48
605B7E98 40
605B7EDC 40
60C659D4 40
605B7E70 32
605B7EB4 32
60616750 24
```

**show memory debug leaks summary Command Example**

The following example shows output from the `show memory debug leaks summary` command:

```
Router# show memory debug leaks summary
Adding blocks for GD...
- **PCI memory**
  - Alloc PC Size Blocks Bytes What
  - I/O memory
  - Processor memory

Alloc PC Size Blocks Bytes What
0x605B7E70 0000000032 0000000001 0000000032 Init
0x605B7E98 0000000040 0000000001 0000000040 Init
0x605B7EB4 0000000032 0000000001 0000000032 Init
0x605B7EDC 0000000040 0000000001 0000000040 Init
0x60616750 0000000024 0000000001 0000000024 Init
0x606167A0 0000000024 0000000001 0000000024 Init
0x608D2848 0000032776 0000000001 0000032776 Audit Process
0x608D2FD8 0000032776 0000000001 0000032776 Audit Process
0x60C656AC 0000000040 0000000001 0000000040 Init
```
The table below describes the significant fields shown in the display.

**Table 108: show memory debug leaks summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alloc_pc</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the leaked block.</td>
</tr>
<tr>
<td>Blocks</td>
<td>Number of blocks leaked.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Total amount of memory leaked.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns the block.</td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500e Series Switches running IOS XE software

**show memory debug leaks all detailed Command Example**

The following example shows output from the `show memory debug leaks all detailed` command:

```
Device# show memory debug leaks all detailed
Process PID : 4644  Process Name : platformmgr
Address    Size Alloc PC TID Name
1FEA5E30   20 00000000000000000000000000000000-0+1F5E51BC 4644 XOS_MEM_XDT
```

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

**Table 109: show memory debug leaks all detailed Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the leaked block.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the leaked block (in bytes).</td>
</tr>
<tr>
<td>Alloc_pc</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>PID</td>
<td>The process identifier of the process that allocated the block.</td>
</tr>
<tr>
<td>TID</td>
<td>The Task identifier for a particular process identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the process that owns the block.</td>
</tr>
</tbody>
</table>
show memory debug leaks all totals Command Example

The following example shows output from the `show memory debug leaks all totals` command:

```
Device# show memory debug leaks all totals

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Num Leak</th>
<th>Total Leak</th>
<th>Num Leak</th>
<th>Total Leak</th>
<th>Total Leak</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mem Blks</td>
<td>Mem Blks(b)</td>
<td>Chunk El</td>
<td>Chunk Elem(b)</td>
<td>(bytes)</td>
</tr>
<tr>
<td>slproc</td>
<td>7</td>
<td>232</td>
<td>0</td>
<td>0</td>
<td>232</td>
</tr>
<tr>
<td>platformmgr</td>
<td>1</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>ns_oir_prox</td>
<td>8</td>
<td>240</td>
<td>0</td>
<td>0</td>
<td>240</td>
</tr>
<tr>
<td>profiled</td>
<td>13</td>
<td>1516</td>
<td>0</td>
<td>0</td>
<td>1516</td>
</tr>
<tr>
<td>obfld</td>
<td>5</td>
<td>1464</td>
<td>9</td>
<td>152</td>
<td>1616</td>
</tr>
<tr>
<td>consoled</td>
<td>13</td>
<td>1516</td>
<td>0</td>
<td>0</td>
<td>1516</td>
</tr>
<tr>
<td>csprovider</td>
<td>13</td>
<td>1552</td>
<td>0</td>
<td>0</td>
<td>1552</td>
</tr>
<tr>
<td>system_mgr</td>
<td>13</td>
<td>1560</td>
<td>0</td>
<td>0</td>
<td>1560</td>
</tr>
<tr>
<td>plogd</td>
<td>7</td>
<td>1736</td>
<td>25</td>
<td>968</td>
<td>2704</td>
</tr>
<tr>
<td>psdprov</td>
<td>13</td>
<td>1532</td>
<td>0</td>
<td>0</td>
<td>1532</td>
</tr>
<tr>
<td>psdtd</td>
<td>16</td>
<td>1564</td>
<td>0</td>
<td>0</td>
<td>1564</td>
</tr>
<tr>
<td>gold_slave</td>
<td>9</td>
<td>376</td>
<td>0</td>
<td>0</td>
<td>376</td>
</tr>
<tr>
<td>osinfo-prov</td>
<td>13</td>
<td>1576</td>
<td>0</td>
<td>0</td>
<td>1576</td>
</tr>
<tr>
<td>oscore_p</td>
<td>13</td>
<td>1520</td>
<td>0</td>
<td>0</td>
<td>1520</td>
</tr>
<tr>
<td>netd</td>
<td>10</td>
<td>256</td>
<td>1</td>
<td>28</td>
<td>284</td>
</tr>
<tr>
<td>mem_mgmt</td>
<td>82</td>
<td>4620</td>
<td>1</td>
<td>40</td>
<td>4660</td>
</tr>
<tr>
<td>mgmte_tap</td>
<td>9</td>
<td>376</td>
<td>0</td>
<td>0</td>
<td>376</td>
</tr>
<tr>
<td>licensed</td>
<td>133</td>
<td>16052</td>
<td>95</td>
<td>2660</td>
<td>18712</td>
</tr>
</tbody>
</table>
```

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

**Table 110: show memory debug leaks all totals Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Name</td>
<td>Name of the leak process.</td>
</tr>
<tr>
<td>Num Leak Mem Blks</td>
<td>Number of memory blocks affected by leak for a particular process.</td>
</tr>
<tr>
<td>Total Leak Mem Blks(b)</td>
<td>Amount of memory affected by leaks in bytes for a particular process.</td>
</tr>
<tr>
<td>Num Leak Chunk El</td>
<td>Number of chunk blocks affected by leak for a particular process.</td>
</tr>
<tr>
<td>Total Leak Chunk Elem(b)</td>
<td>Amount of chunk block memory affected by leaks in bytes for a particular process.</td>
</tr>
<tr>
<td>Total Leak (bytes)</td>
<td>Total amount of memory leaked for a particular process.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set memory debug incremental starting-time</td>
<td>Sets the current time as the starting time for incremental analysis.</td>
</tr>
<tr>
<td>show memory debug incremental allocation</td>
<td>Displays all memory blocks that were allocated after the issue of the set memory debug incremental starting-time command.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show memory debug incremental leaks</code></td>
<td>Displays only memory that was leaked after the issue of the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td><code>show memory debug incremental leaks lowmem</code></td>
<td>Forces incremental memory leak detection to work in low memory mode. Displays only memory that was leaked after the issue of the <code>set memory debug incremental starting-time</code> command.</td>
</tr>
<tr>
<td><code>show memory debug incremental status</code></td>
<td>Displays if the starting point of incremental analysis has been defined and the time elapsed since then.</td>
</tr>
</tbody>
</table>

### show memory debug references

To display debug information on references, use the `show memory debug references` command in user EXEC or privileged EXEC mode.

**Syntax Description**

```
show memory debug references [dangling [start-address start-address]]
```

**dangling** (Optional) Displays the possible references to free memory.

**start-address** (Optional) Address numbers <0-4294967295> that determine the address range.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

All show memory debug commands must be used on customer networks only to diagnose the router for memory leaks when memory depletion is observed. These CLI’s will have high CPU utilization and might result in time sensitive protocols to flap. These CLI’s are recommended for customer use, only in the maintenance window when the router is not in a scaled condition.

**Examples**

The following is sample output from the `show memory debug references` command:

```
Router# show memory debug references 2 3
Address Reference Cont_block Cont_block_name
442850BC 2 44284960 bss
44285110 3 44284960 bss
4429c33c 2 44284960 bss
4429c34c 2 44284960 bss
4429c35c 3 44284960 bss
```

The following is sample output from the `show memory debug references dangling` command:

```
Router# show memory debug references dangling
Address Reference Free_block Cont_block Cont_block_name
```
The table below describes the significant fields shown in the displays.

### Table 111: show memory debug references Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block having the given or dangling reference.</td>
</tr>
<tr>
<td>Reference</td>
<td>Address which is given or dangling.</td>
</tr>
<tr>
<td>Free_block</td>
<td>Address of the free block which now contains the memory referenced by the dangling reference.</td>
</tr>
<tr>
<td>Cont_block</td>
<td>Address of the control block which contains the block having the reference.</td>
</tr>
<tr>
<td>Cont_block_name</td>
<td>Name of the control block.</td>
</tr>
</tbody>
</table>

### show memory debug unused

To display debug information on leaks that are accessible, but are no longer needed, use the `show memory debug unused` command in user EXEC or privileged EXEC mode.

**show memory debug unused**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show memory debug unused` command:

```
Router# show memory debug unused
Address Alloc_pc PID size Name
654894B8 62BF31DC -2 44 *Init*
6549A074 601F7A84 -2 4464 XDI data
6549B218 601F7274 -2 4500 XDI data
6549DFB0 6089DDA4 42 84 Init
65509160 6089DDA4 1 84 *Init*
6550A260 6089DDA4 2 84 *Init*
6551FDB4 6089DDA4 4 84 *Init*
6551FF34 627EFA2C -2 24 *Init*
65520B3C 6078B1A4 -2 24 Parser Mode Q1
```
show memory detailed

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

Table 112: show memory debug unused Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Alloc_pc</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier of the process that allocated the block.</td>
</tr>
<tr>
<td>size</td>
<td>Size of the unused block (in bytes).</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the process that owns the block.</td>
</tr>
</tbody>
</table>

**show memory detailed**

To display detailed memory information about POSIX and Cisco IOS processes when Cisco IOS XE or Software Modularity images are running, use the **show memory detailed** command in privileged EXEC mode.

**Cisco IOS Software Modularity**

```
show memory detailed [{process-id}process-name} [{start-address
[end-address]bigger|free|physical|shared|statistics|summary}]
```

**Cisco Catalyst 4500e Series Switches running IOS XE software**

```
show memory detailed [{process {process-id}process-name}|free|io|overflow|statistics|summary}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) POSIX process identifier.</td>
</tr>
<tr>
<td>process-name</td>
<td>(Optional) POSIX process name.</td>
</tr>
<tr>
<td>start-address</td>
<td>(Optional) Starting memory address.</td>
</tr>
<tr>
<td>end-address</td>
<td>(Optional) Ending memory address.</td>
</tr>
<tr>
<td>bigger</td>
<td>(Optional) Displays information about bigger free blocks in the process.</td>
</tr>
</tbody>
</table>
**show memory detailed**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>free</td>
<td>(Optional) Displays free memory information.</td>
</tr>
<tr>
<td>io</td>
<td>(Optional) Displays the free I/O memory blocks.</td>
</tr>
<tr>
<td>overflow</td>
<td>(Optional) Displays details about memory block header corruption corrections when the exception memory ignore overflow global configuration command is configured.</td>
</tr>
<tr>
<td>physical</td>
<td>(Optional) Displays physical memory information.</td>
</tr>
<tr>
<td>shared</td>
<td>(Optional) Displays shared memory information.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Displays detailed memory usage by address of the system call that allocated the block.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays summary information about memory usage per system call that allocated the block.</td>
</tr>
</tbody>
</table>

**Command Default**

No detailed memory information about POSIX and Cisco IOS processes is displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXF4</td>
<td>This command was introduced to support Software Modularity images.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1.0.SG</td>
<td>This command was introduced on the Cisco Catalyst 4500e Serfies Switches.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Detailed output of the process memory on the device is displayed with this command. The process memory summary is displayed first, followed by POSIX and Cisco IOS memory information. The POSIX memory information includes the address, the size in bytes, and the type of memory used by various segments such as program text, data, stack, shared memory, device memory, and heap. Cisco IOS memory information includes the native Cisco IOS display of memory blocks maintained by the Cisco IOS memory management library.

**Cisco IOS Software**

The following is partial sample output from the `show memory detailed` command for a Cisco IOS process:

```
Router# show memory detailed cdp2.iosproc
System Memory: 131072K total, 115836K used, 15236K free 4000K kernel reserved
Process sbin/cdp2.iosproc, type IOS, PID = 12329
  636K total, 4K text, 4K data, 28K stack, 600K dynamic
  16384 heapsize, 3972 allocated, 10848 free
Address Bytes What
0x3B42000 4194304 Shared Memory
0x7FBB000 8192 Program Stack
0x8020000 49152 Program Text
0x802C000 4096 Program Data
0x802D000 8192 Allocated memory
0x60000000 4096 Shared Memory "SHM_IDB"
0x60001000 32768 Shared Memory
```
The first section of the display shows system summary information. The table below describes the significant fields shown in the first section of the display.

**Table 113: show memory detailed Field Descriptions--First Section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>Total amount of memory on the device, in kilobytes.</td>
</tr>
<tr>
<td>used</td>
<td>Amount of memory in use, in kilobytes.</td>
</tr>
<tr>
<td>free</td>
<td>Amount of memory not in use, in kilobytes.</td>
</tr>
<tr>
<td>kernel reserved</td>
<td>Amount of memory reserved by the kernel, in kilobytes.</td>
</tr>
</tbody>
</table>

The second section of the display includes process summary statistics about the activities of the system memory allocator. The table below describes the significant fields shown in the second section of the display.

**Table 114: show memory detailed Field Descriptions--Second Section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Process name and path.</td>
</tr>
<tr>
<td>type</td>
<td>Type of process: POSIX or IOS.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>total</td>
<td>Total amount of memory used by the specified process, in kilobytes.</td>
</tr>
<tr>
<td>text</td>
<td>Amount of memory, in kilobytes, used by the text segment of the specified process.</td>
</tr>
<tr>
<td>data</td>
<td>Amount of memory, in kilobytes, used by the data segment of the specified process.</td>
</tr>
<tr>
<td>stack</td>
<td>Amount of memory, in kilobytes, used by the stack segment of the specified process.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Amount of memory, in kilobytes, used by the dynamic segment of the specified process.</td>
</tr>
<tr>
<td>heapsize</td>
<td>Size of the process heap. Note that the Cisco IOS memory management library allocates heap dynamically. This is shown in the Cisco IOS memory details that follow the POSIX memory display.</td>
</tr>
<tr>
<td>allocated</td>
<td>Amount of memory, in kilobytes, allocated from the heap.</td>
</tr>
<tr>
<td>free</td>
<td>Amount of free memory, in kilobytes, in the heap for the specified process.</td>
</tr>
</tbody>
</table>
The third section of the display shows POSIX process perspective memory information. The table below describes the significant fields shown in the third section of the display.

**Table 115: show memory detailed Field Descriptions--Third Section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of block (in bytes).</td>
</tr>
<tr>
<td>What</td>
<td>Type of memory segment that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>

The fourth section of the display shows Cisco IOS memory information as a block-by-block listing of memory use. The table below describes the significant fields shown in the fourth section of the display.

**Table 116: show memory detailed Field Descriptions--Fourth Section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>Hexadecimal address of the head of the memory allocation chain.</td>
</tr>
<tr>
<td>Total(b)</td>
<td>Sum of used bytes plus free bytes.</td>
</tr>
<tr>
<td>Used(b)</td>
<td>Amount of memory in use.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of memory not in use.</td>
</tr>
<tr>
<td>Lowest(b)</td>
<td>Smallest amount of free memory since last boot.</td>
</tr>
<tr>
<td>Largest(b)</td>
<td>Size of largest available free block.</td>
</tr>
<tr>
<td>Address</td>
<td>Hexadecimal address of block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of block (in bytes).</td>
</tr>
<tr>
<td>Prev</td>
<td>Address of previous block (should match address on previous line).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of next block (should match address on next line).</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of previous free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of next free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>what</td>
<td>Type of memory segment that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show memory detailed` command for a POSIX process:

```
Router# show memory detailed 12290
System Memory: 131072K total, 115876K used, 15196K free 4000K kernel reserved
```
Process sbin/sysmgr.proc, type POSIX, PID = 12290
  400K total, 100K text, 144K data, 12K stack, 144K dynamic
  81920 heapsize, 6816 allocated, 8824 free

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x7FDF000</td>
<td>126976</td>
<td>Program Stack (pages not allocated)</td>
</tr>
<tr>
<td>0x7FEE000</td>
<td>4096</td>
<td>Program Stack</td>
</tr>
<tr>
<td>0x8000000</td>
<td>122880</td>
<td>Program Stack (pages not allocated)</td>
</tr>
<tr>
<td>0x801E000</td>
<td>8192</td>
<td>Program Stack</td>
</tr>
<tr>
<td>0x8020000</td>
<td>102400</td>
<td>Program Text</td>
</tr>
<tr>
<td>0x8039000</td>
<td>147456</td>
<td>Program Data</td>
</tr>
<tr>
<td>0x805D000</td>
<td>8192</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8060000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8064000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8068000</td>
<td>8192</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x806C000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8070000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8074000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8078000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x807C000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
<tr>
<td>0x8080000</td>
<td>16384</td>
<td>Heap Memory</td>
</tr>
</tbody>
</table>

The following partial sample output from the `show memory detailed` command with a process name and the `physical` keyword that displays the summary of physical memory used by the specified process along with the shared memory details:

```
Router# show memory detailed sysmgr.proc physical
Pid     Data    Stack    Dynamic    Text    Shared    Maps    Process
20482   304K    16K      256K       3480K   468K      60      sysmgr.proc

Total Physical Memory used or mapped by sysmgr.proc
  Private memory used (Data/Stack/Dynamic) : 576K
  Shared memory mapped (Text/Shared) : 3948K
  Number of memory maps : 60

Dev 1:Text/Data 2:Mapped 3:Shared 4:DSO
LZY:Lazy ELF:Elf STK:Stack NOC:Nocache

<table>
<thead>
<tr>
<th>Phy Addr</th>
<th>Size</th>
<th>Pid</th>
<th>Virt Addr</th>
<th>What</th>
<th>Dev</th>
<th>Prot</th>
<th>MapFlags</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>32768K</td>
<td>20482</td>
<td>0x7000000</td>
<td>Text</td>
<td>4</td>
<td>X</td>
<td>SHD FXD ELF</td>
</tr>
<tr>
<td>0x2000000</td>
<td>32768K</td>
<td>20482</td>
<td>0x7200000</td>
<td>Text</td>
<td>4</td>
<td>X</td>
<td>SHD FXD ELF</td>
</tr>
<tr>
<td>0x4000000</td>
<td>32768K</td>
<td>20482</td>
<td>0x7400000</td>
<td>Text</td>
<td>4</td>
<td>X</td>
<td>SHD FXD ELF</td>
</tr>
<tr>
<td>0x522B000</td>
<td>4K</td>
<td>20482</td>
<td>0x1020000</td>
<td>Text</td>
<td>4</td>
<td>X</td>
<td>SHD FXD ELF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phy Addr</th>
<th>Size</th>
<th>Pid</th>
<th>Virt Addr</th>
<th>What</th>
<th>Dev</th>
<th>Prot</th>
<th>MapFlags</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x9EFD4000</td>
<td>32K</td>
<td>20482</td>
<td>0x105C000</td>
<td>Heap</td>
<td>2</td>
<td>RW-</td>
<td>PRV ANN</td>
</tr>
<tr>
<td>0x9EF00000</td>
<td>32K</td>
<td>20482</td>
<td>0x1054000</td>
<td>Heap</td>
<td>2</td>
<td>RW-</td>
<td>PRV ANN</td>
</tr>
<tr>
<td>0x9EF80000</td>
<td>32K</td>
<td>20482</td>
<td>0x1034000</td>
<td>Heap</td>
<td>2</td>
<td>RW-</td>
<td>PRV ANN</td>
</tr>
<tr>
<td>0x9F003000</td>
<td>4K</td>
<td>20482</td>
<td>0x7B43C000</td>
<td>Data</td>
<td>4</td>
<td>RW-</td>
<td>PRV FXD ANN ELF</td>
</tr>
</tbody>
</table>
```

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

**Table 117: show memory detailed Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
<td>Amount of memory shared by the specified process, in kilobytes.</td>
</tr>
<tr>
<td>Maps</td>
<td>Number of memory maps for the specified process.</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>Private memory used</td>
<td>Total amount of private memory used by the process.</td>
</tr>
</tbody>
</table>
**Cisco Catalyst 4500e Series Switches running IOS XE software**

The following is sample output from the `show memory detailed` command for the `iosd` process:

```
Switch#show memory detailed proc iosd
System memory : 883144K total, 591378K used, 291766K free, 165432K kernel reserved
Lowest(b) : 5128192
Process iosd, type L, PID = 11007
  777572K total, 82212K text, 537120K data, 84K stack, 240K dynamic
  240 heapsize, 240 allocated, 0 free
  Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
  Processor 90150008 536870912 261852128 275018784 273655520 272592492
  I/O  B0151000 16777216 169288 16607928 16598952 16598948
  Processor memory
  Address Bytes Prev Next Ref PrevF NextF Alloc PC what
  90150008 0000000436 00000000 901501E8 001 --------- 10280C10  *Init*
  901501E8 0000020004 90150008 90155038 001 --------- 11D5E9D4 Managed Chunk Queue
```
show memory ecc

To display single-bit Error Code Correction (ECC) error logset data, use the show memory ecc command in privileged EXEC mode.

show memory ecc

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory</td>
<td>Displays system memory information.</td>
</tr>
<tr>
<td>show memory detailed all</td>
<td>Displays detailed memory information of all applicable processes.</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1(30)CC</td>
<td>This command was introduced in Cisco IOS Release 11.1(30)CC.</td>
</tr>
<tr>
<td>12.0(4)XE</td>
<td>This command was integrated into Cisco IOS Release 12.0(4)XE.</td>
</tr>
<tr>
<td>12.0(6)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(6)S.</td>
</tr>
<tr>
<td>12.1(13)</td>
<td>This command was integrated into Cisco IOS Release 12.1(13).</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to determine if the router has experienced single-bit parity errors.

Examples

The following is sample output from the show memory ecc command from a 12000-series router running Cisco IOS Release 12.0(23)S:

Router# show memory ecc
ECC Single Bit error log
------------------------
Single Bit error detected and corrected at 0x574F3640
 - Occured 1 time(s)
 - Whether a scrub was attempted at this address: Yes
 - Syndrome of the last error at this address: 0xE9
 - Error detected on a read-modify-write cycle ? No
 - Address region classification: Unknown
 - Address media classification : Read/Write
  Single Bit error detected and corrected at 0x56AB3760
 - Occured 1 time(s)
 - Whether a scrub was attempted at this address: Yes
 - Syndrome of the last error at this address: 0x68
 - Error detected on a read-modify-write cycle ? No
 - Address region classification: Unknown
 - Address media classification : Read/Write
Total Single Bit error(s) thus far: 2

The table below describes the significant fields shown in the first section of the display.

Table 118: show memory ecc Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occured n time(s)</td>
<td>Number of single-bit errors that has occurred.</td>
</tr>
<tr>
<td>Whether a scrub was attempted at this address:</td>
<td>Indicates whether a scrub has been performed.</td>
</tr>
<tr>
<td>Syndrome of the last error at this address:</td>
<td>Describes the syndrome of last error.</td>
</tr>
<tr>
<td>Error detected on a read-modify-write cycle ?</td>
<td>Indicates whether an error has occurred.</td>
</tr>
<tr>
<td>Address region classification: Unknown</td>
<td>Describes the region of the error.</td>
</tr>
<tr>
<td>Address media classification :</td>
<td>Describes the media of the error and correction.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory</td>
<td>Displays statistics about memory, including memory-free pool statistics.</td>
</tr>
</tbody>
</table>
show memory events

To display recorded memory events, use the `show memory events` command in privileged EXEC mode.

```
show memory events [outstanding [summary]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outstanding</td>
<td>(Optional) Displays the outstanding allocation events in the event buffer.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of outstanding allocation events in the event buffer.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can enable the `show memory events` command, you must configure the `memory record events` command in global configuration mode.

**Examples**

The following is sample output from the `show memory events` command:

```
Router# configure terminal
Router(config)# memory record events
Memory event recording already enabled!
Router(config)# exit
Router# show memory events
Last recorded memory events:
When Type Block/Chunk DataPtr Size PID What Traceback/PC
4d19h FREE 695B3200 695B3230 3000 82 Iterator Hash Entry 615B75C4
```

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

**Table 119: show memory events Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Time when the memory event was last seen by the system (in hours and days).</td>
</tr>
<tr>
<td>Type</td>
<td>Allocation type.</td>
</tr>
<tr>
<td>Block/Chunk/DataPtr</td>
<td>Number of memory events allocated.</td>
</tr>
<tr>
<td>Size</td>
<td>Amount of memory, in bytes, used by the task.</td>
</tr>
<tr>
<td>PID</td>
<td>Packet identification number.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns a block or fragment.</td>
</tr>
<tr>
<td>Traceback/PC</td>
<td>Traceback error.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show memory events` command using the `outstanding and summary` keywords:
Router# configure terminal
Router(config)# memory record events
Memory event recording already enabled!
Router(config)# exit
Router# show memory events outstanding summary

<table>
<thead>
<tr>
<th>Last-Seen</th>
<th>Type</th>
<th>How-Many</th>
<th>Size</th>
<th>PID</th>
<th>What</th>
<th>Traceback/PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>5d16h</td>
<td>ALLOC</td>
<td>1</td>
<td>320</td>
<td>135</td>
<td>Exec</td>
<td>61B399F4</td>
</tr>
</tbody>
</table>

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

**Table 120: show memory events Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last-Seen</td>
<td>Time when the memory event was last seen by the system (in hours and days).</td>
</tr>
<tr>
<td>Type</td>
<td>Allocation type.</td>
</tr>
<tr>
<td>How-Many</td>
<td>Number of memory events allocated.</td>
</tr>
<tr>
<td>Size</td>
<td>Amount of memory, in bytes, used by the task.</td>
</tr>
<tr>
<td>PID</td>
<td>Packet identification number.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns a block or fragment.</td>
</tr>
<tr>
<td>Traceback/PC</td>
<td>Traceback error.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory traceback</td>
<td>Displays memory traceback information.</td>
</tr>
</tbody>
</table>

**show memory failures alloc**

To display statistics about failed memory allocation requests, use the **show memory failures alloc** command in the privileged EXEC mode.

```
show memory failures alloc
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **show memory failures alloc** command:
Router# show memory failures alloc

<table>
<thead>
<tr>
<th>Caller</th>
<th>Pool</th>
<th>Size</th>
<th>Alignment</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
<tr>
<td>0x60394744</td>
<td>I/O</td>
<td>1684</td>
<td>32</td>
<td>00:10:03</td>
</tr>
</tbody>
</table>

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

**Table 121: show memory failures alloc Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td>Address of the allocator function that issued memory allocation request that failed.</td>
</tr>
<tr>
<td>Pool</td>
<td>Pool from which the memory was requested.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the memory requested in bits.</td>
</tr>
<tr>
<td>Alignment</td>
<td>Memory alignment in bits.</td>
</tr>
<tr>
<td>When</td>
<td>Time of day at which the memory allocation request was issued.</td>
</tr>
</tbody>
</table>

**show memory fast**

To display fast memory details for the router, use the **show memory fast** command.

```
show memory fast [{allocating-process | totals|dead | totals|free  | totals}]
```

**Syntax Description**

- **allocating-process** (Optional) Include allocating process names with the standard output.
- **dead** (Optional) Display only memory owned by dead processes.
- **free** (Optional) Display only memory not allocated to a process.
- **totals** (Optional) Summarizes the statistics for allocating processes, dead memory, or free memory.

**Command Modes**

Exec

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced in a release prior to 12.1. This command replaced the <strong>show memory sram</strong> command.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The show memory fast command displays the statistics for the fast memory. “Fast memory” is another name for “processor memory,” and is also known as “cache memory.” Cache memory is called fast memory because the processor can generally access the local cache (traditionally stored on SRAM positioned close to the processor) much more quickly than main memory or RAM.

Note

The show memory fast command is a command alias for the show memory processor command. These commands will issue the same output.

Examples

The following example shows sample output from the show memory fast and the show memory processor commands:

```
Router> show memory fast

Processor memory
Address     Bytes Prev Next Ref PrevF NextF Alloc PC what
8404A580 0001493284 00000000 841B6ECC 000 0 84BADF88 815219D8 (coalesced)
841B6ECC 0000020004 8404A580 841BBD18 001 -------- -------- 815DB094 Managed Chunk Queue Elements
841BBD18 0000001504 841B6ECC 841B3C20 001 -------- -------- 8159EAC4 List Elements
841B3C20 0000005004 841BBD18 841BD6D4 001 -------- -------- 8159EB04 List Headers
841BD6D4 0000000048 841B3C20 841BD72C 001 -------- -------- 8152A614 *Init*
841BD72C 0000001504 841BD6D4 841BD34 001 -------- -------- 815A9514 messages
841BD34 0000001504 841BD72C 841BE3C 001 -------- -------- 815A9540 Watched messages
841BE3C 0000001504 841BD34 841BE944 001 -------- -------- 815A95E4 Watched Semaphore
841BE944 0000000504 841BE3C 841BE6D4 001 -------- -------- 815A9630 Watched Message Queue
841BE6D4 0000001504 841BE944 841BF16C 001 -------- -------- 815A9658 Watcher Message Queue
841BF16C 00000001036 841BE6D4 841BF5A0 001 -------- -------- 815A2B24 Process Array
-- More --
<Ctrl+z>

Router> show memory processor

Processor memory
Address     Bytes Prev Next Ref PrevF NextF Alloc PC what
8404A580 0001493284 00000000 841B6ECC 000 0 84BADF88 815219D8 (coalesced)
841B6ECC 0000020004 8404A580 841BBD18 001 -------- -------- 815DB094 Managed Chunk Queue Elements
841BBD18 0000001504 841B6ECC 841B3C20 001 -------- -------- 8159EAC4 List Elements
841B3C20 0000005004 841BBD18 841BD6D4 001 -------- -------- 8159EB04 List Headers
841BD6D4 0000000048 841B3C20 841BD72C 001 -------- -------- 8152A614 *Init*
841BD72C 0000001504 841BD6D4 841BD34 001 -------- -------- 815A9514 messages
841BD34 0000001504 841BD72C 841BE3C 001 -------- -------- 815A9540 Watched messages
841BE3C 0000001504 841BD34 841BE944 001 -------- -------- 815A95E4 Watched Semaphore
841BE944 0000000504 841BE3C 841BE6D4 001 -------- -------- 815A9630 Watched Message Queue
841BE6D4 0000001504 841BE944 841BF16C 001 -------- -------- 815A9658 Watcher Message Queue
841BF16C 00000001036 841BE6D4 841BF5A0 001 -------- -------- 815A2B24 Process Array
-- More --
<Ctrl+z>

Router>
```

The following example shows sample output from the show memory fast allocating-process command, followed by sample output from the show memory fast allocating-process totals command:

```
Router> show memory fast allocating-process

Processor memory
```

Cisco IOS Configuration Fundamentals Command Reference
show memory fragment

The following example shows sample output from the `show memory fast dead` command:

```
Router# show memory fast dead

Processor memory
Address Bytes Prev Next Ref PrevF NextF Alloc PC what
8498FC20 0000000028 8498FB90 8498FC64 001 -------- ------- 81472B24 AAA MI SG NAME
--------
68

Router# show memory fast dead totals

Dead Proc Summary for: Processor
PC Total Count Name
0x81472B24 68 1 AAA MI SG NAME
```

to display the block details of fragmented free blocks and allocated blocks, which is physically just before or after the blocks on the free list, use the `show memory fragment` command in user EXEC or privileged EXEC mode.

```
show memory [{processor|io}] fragment [detail]
```
## Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processor</td>
<td>(Optional) Displays the processor memory information.</td>
</tr>
<tr>
<td>io</td>
<td>(Optional) Displays the I/O memory information.</td>
</tr>
<tr>
<td>fragment</td>
<td>Displays the information of the free blocks and the blocks surrounding the free blocks.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the detailed information of all the free blocks and the blocks surrounding the free blocks that are located between the allocated blocks.</td>
</tr>
</tbody>
</table>

## Command Modes

User EXEC Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
</tbody>
</table>

## Examples

The following is sample output from the `show memory processor fragment` command:

```plaintext
Router# show memory processor fragment
Processor memory
Free memory size : 65516944 Number of free blocks: 230
Allocated PC Summary for allocated blocks in pool: Processor
PC Total Count Name
0x6047DDCC 852020 1 atmdx_vc_table
0x6075DC30 544392 4 ATM1/0
0x61BDBA14 131176 2 eddri_self_event
0x61913BEC 131124 1 l2tp_tnl_table
0x602E9820 114832 1 AutoVC Msg Chunk
0x6071253C 98408 2 Exec
0x607DF5BC 96624 12 Process Stack
0x6118DDA0 77252 1 Spanning Tree Opt Port Block
0x61F13C30 67636 1 QOS_MODULE_MAIN
0x6047DD3C 65640 2 atmdx_tx_shadow
0x614B6624 65588 1 CEF: loadinfo chunk
0x614D1924 65588 1 IP mtrie node
0x619241D4 65588 1 PPTP mgd timer chunk
0x606581CC 65588 1 AAA DB Chunk
0x607E5EAC 65588 1 MallocLite
0x6192420C 65588 1 PPTP: pptp_tunneltype chunk
0x6075DCB8 45924 10 FastEthernet2/ |
0x607CA400 36288 2 pak_subblock chunk
0x6255648C 28948 1 CCPROXY_CT
0x6047DE0C 16432 17 TCP CB
0x6192420C 65588 1 AC context chunks
0x6192420C 65588 1 AC Mgr mgd timer chunk
0x60734010 16644 19 *Packet Header*
0x6047DE0C 16436 1 atmdx_abr_stats
0x6047DCC 16112 2 atmdx_rx_pool_info
0x60A77E98 13060 1 DHCPD Message Workspace
0x61F50008 12852 1 CCVPM_HTS
0x61F50008 12852 1 Virtual Exec
0x60EFA1EC 12344 1 RSVP DB Handle Bin
```
The following is sample output from the `show memory processor fragment detail` command:

```
Router# show memory processor fragment detail

Processor memory
Free memory size : 65566148 Number of free blocks: 230

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>Prev</th>
<th>Next</th>
<th>Ref</th>
<th>PrevF</th>
<th>NextF</th>
<th>Alloc</th>
<th>PC</th>
<th>what</th>
</tr>
</thead>
<tbody>
<tr>
<td>645A8148</td>
<td>0000000028</td>
<td>645A80F0</td>
<td>645A8194</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>60695B20</td>
<td>Init</td>
<td></td>
</tr>
<tr>
<td>645A8194</td>
<td>0000000040</td>
<td>645A8148</td>
<td>645A818C</td>
<td>000</td>
<td>0</td>
<td>200B4300</td>
<td>606B9614</td>
<td>NameDB String</td>
<td></td>
</tr>
<tr>
<td>645A81BC</td>
<td>0000000260</td>
<td>645A8194</td>
<td>645A8320</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>607C2D20</td>
<td>Init</td>
<td></td>
</tr>
<tr>
<td>200B4300</td>
<td>0000000028</td>
<td>200B42B4</td>
<td>200B434C</td>
<td>000</td>
<td>645A8194</td>
<td>6490F7E8</td>
<td>60976574</td>
<td>AAA Event Data</td>
<td></td>
</tr>
<tr>
<td>200B434C</td>
<td>0000000200</td>
<td>200B4300</td>
<td>200B4B50</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>6267D294</td>
<td>Coproc Request Structures</td>
<td></td>
</tr>
<tr>
<td>6490F79C</td>
<td>0000000028</td>
<td>6490F748</td>
<td>6490F7E8</td>
<td>001</td>
<td>------</td>
<td>------</td>
<td>606DDA04</td>
<td>Parser Linkage</td>
<td></td>
</tr>
<tr>
<td>6490F7E8</td>
<td>0000000028</td>
<td>6490F79C</td>
<td>6490F834</td>
<td>000</td>
<td>200B4300</td>
<td>6491120C</td>
<td>606DD8D8</td>
<td>Init</td>
<td></td>
</tr>
</tbody>
</table>
```

show memory lite-chunks

To display statistics about malloc-lite memory, use the show memory lite-chunks command in user EXEC or privileged EXEC mode

```
show memory lite-chunks {statistics|totals} {summary|pool|{all|pool}}
```

**Syntax Description**

- **statistics** Displays malloc lite utilization statistics sorted by pool.
- **totals** Displays malloc lite allocating totals.
- **summary** Displays a summary of malloc lite usage for all or a specific pool.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory io</td>
<td>Configures thresholds for I/O memory.</td>
</tr>
<tr>
<td>memory processor</td>
<td>Configures thresholds for processor memory.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show memory lite-chunks` command.

```
Device# show memory lite-chunks pool 8

   8 bytes pool

  Address  Ref   Alloc PC
  69D0CCBC 000   64286AAC
  69D0CCD8 000   64286AAC
  69D0CCF4 000   64286AAC
  69D0CD10 000   64286AAC
  69D0CD2C 000   64286AAC
  69D0CD48 000   64286AAC
  69D0CD64 000   64286AAC
  69D0CD80 000   64286AAC
  69D0CD9C 000   64286AAC
  69D0CDB8 000   64286AAC
  69D0CDD4 000   64286AAC
  69D0CDF0 000   64286AAC
  69D0CE0C 000   64286AAC
  69D0CE28 000   64286AAC
  69D0CE44 000   64286AAC
  69D0CE60 000   64286AAC
  69D0CE7C 000   64286AAC
  69D0CE98 000   64286AAC
  69D0CEB4 000   64286AAC
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
</tbody>
</table>
show memory multibus

To display statistics about multibus memory, including memory-free pool statistics, use the `show memory multibus` command in user EXEC or privileged EXEC mode.

```
show memory multibus [ { allocating-process [ totals ] | dead [ totals ] | free [ totals ] } ]
```

**Syntax Description**

- `allocating-process [ totals ]`: (Optional) Displays allocating memory totals by name.
- `dead [ totals ]`: (Optional) Displays memory totals on dead processes.
- `free [ totals ]`: (Optional) Displays statistics on free memory.
- `statistics [ history ]`: (Optional) Displays memory pool history statistics on all processes.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show memory multibus` command:

```
Router# show memory multibus
Processor memory

Address Bytes Prev Next Ref PrevF NextF Alloc PC what
6540BBA0 0000016388 00000000 6540FBD4 001 -------- 60883984 TW Buckes
6540FBD4 0000016388 6540BBA0 65413C08 001 -------- 60883984 TW Buckes
65413C08 0000016388 6540FBD4 65417C3C 001 -------- 60883984 TW Buckes
65417C3C 0000006004 65413C08 654193E0 001 -------- 608A0D4C Process k
654193E0 0000012004 65417C3C 6541C2F4 001 -------- 608A0D4C Process k
6541C2F4 0000411712 654193E0 65480B64 000 0 0 608A0D4C (fragment)
65480B64 0000020004 6541C2F4 654859B8 001 -------- 608CF99C Managed s
654859B8 0000010004 65480B64 654880FC 001 -------- 6085C7F8 List Eles
654880FC 0000005004 654859B8 654894B8 001 -------- 6085C83C List Heas
654894B8 0000000040 65480B64 65489518 001 -------- 62BF31DC *Init*

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

**Table 123: show memory multibus Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev</td>
<td>Address of the preceding block (should match the address on the preceding line).</td>
</tr>
</tbody>
</table>
show memory pci

To display statistics about Peripheral Component Interconnect (PCI) memory, use the `show memory pci` command in user EXEC or privileged EXEC mode.

**show memory pci**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show memory pci` command:

```
Router# show memory pci
I/O memory
Address Bytes Prev Next Ref PrevF NextF Alloc PC what
0E000000 0000000032 0E000000 0E000050 000 64F5EBF4 0 00000000 (fragmen)
0E000050 00000000272 0E000000 0E000190 001 607E2EC0 *Packet *
0E000190 00000000272 0E000050 0E0002D0 001 607E2EC0 *Packet *
0E0002D0 00000000272 0E000190 0E000410 001 607E2EC0 *Packet *
0E000410 00000000272 0E0002D0 0E000550 001 607E2EC0 *Packet *
0E000550 00000000272 0E000410 0E000690 001 607E2EC0 *Packet *
0E000690 00000000272 0E000550 0E0007D0 001 607E2EC0 *Packet *
0E0007D0 00000000272 0E000690 0E000910 001 607E2EC0 *Packet *
0E000910 00000000272 0E0007D0 0E000A50 001 607E2EC0 *Packet *
0E000A50 00000000272 0E000910 0E000B90 001 607E2EC0 *Packet *
0E000B90 00000000272 0E000A50 0E000CD0 001 607E2EC0 *Packet *
Address Bytes Prev Next Ref PrevF NextF Alloc PC what
0E00CD0 00000000272 0E000B90 0E000E10 001 607E2EC0 *Packet *
0E000E10 00000000272 0E000CD0 0E000F50 001 607E2EC0 *Packet *
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next</td>
<td>Address of the following block (should match the address on the following line).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of the preceding free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of the following free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns the block, or “(fragmen)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>
Table 124: show memory pci Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev</td>
<td>Address of the preceding block (should match the address on the preceding line).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of the following block (should match the address on the following line).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of the preceding free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of the following free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
<tr>
<td>what</td>
<td>Name of process that owns the block, or &quot;(fragmen)&quot; if the block is a fragment, or &quot;(coalesced)&quot; if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>

show memory processor

To display statistics on the Router Processor memory, use the `show memory processor` command in user EXEC or privileged EXEC mode.

```
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allocating-process</td>
<td>(Optional) Displays the allocating process name.</td>
</tr>
<tr>
<td>totals</td>
<td>(Optional) Displays the total allocated memory.</td>
</tr>
<tr>
<td>dead</td>
<td>(Optional) Displays information about memory owned by dead processes.</td>
</tr>
<tr>
<td>totals</td>
<td>(Optional) Displays the total dead process memory.</td>
</tr>
<tr>
<td>fragment</td>
<td>(Optional) Displays the block details of fragmented free blocks and allocated blocks, which are shown either preceding or following the blocks on the free list.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays memory fragment information in detail.</td>
</tr>
<tr>
<td>free</td>
<td>(Optional) Displays memory pool statistics.</td>
</tr>
<tr>
<td>totals</td>
<td>(Optional) Displays the statistics of the available processor memory.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Displays the total free memory.</td>
</tr>
</tbody>
</table>

Command Modes

User EXEC (>) Privileged EXEC (#)
show memory processor

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The <code>allocating-process</code> and <code>dead</code> keywords were added.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the `show memory processor` command:

```
Router# show memory processor
Processor memory
Address  Bytes  Prev  Next  Ref  PrevF  NextF  Alloc  PC  what
6540BBA0 0000016388 00000000 6540FBD4 001  --------  --------  60883984  TW Buckes
6540FBD4 0000016388 6540BBA0 65413C08 001  --------  --------  60883984  TW Buckes
65413C08 0000016388 6540FBD4 65417C3C 001  --------  --------  60883984  TW Buckes
65417C3C 0000060004 65413C08 654193E0 001  --------  --------  608A0D4C  Process k
654193E0 0000120004 65417C3C 65412C7F 001  --------  --------  608A0D4C  Process k
65412C7F 0000117112 654193E0 65480B64 000 0  0  608A0D4C  (fragmen)
65480B64 0000200004 65412C7F 654839B8 001  --------  --------  608CF99C  Managed s
654839B8 0000010004 65480B64 654859B4 001  --------  --------  608A0D4C  Process k
654859B4 0000117112 654839B8 654894B8 001  --------  --------  6085C83C  List Eles
654894B8 0000000004 654859B4 65489518 001  --------  --------  62BF31DC  *Init*
```

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

```
Table 125: show memory processor Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev</td>
<td>Address of the preceding block (should match the address on the preceding line).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of the following block (should match the address on the following line).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of the preceding free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of the following free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns the block or fragment.</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show memory processor allocating-process` command:

```
Router# show memory processor allocating-process
PC  Total  Count  Name
0x6013A948 3719220 1  atmdx_setup_vc_table
0x6064EB28 2581132 291  Process Stack
0x627E2420 2559476 78  CCE dp subloc
0x62A098C8 1637116 24  regex
```
The following is sample output from the `show memory processor dead` command:

```
Router# show memory processor dead

PC  Total  Count  Name
---  ------  ----  -----  
0x61E4EB70  65588  1  IP Static Rout
0x62322A2C  65588  1  MFI: Clnt SMsg
0x6268DFF4  32820  1  PPP Context Ch
0x62660CCC  32820  1  PPP HANDLE IDs
0x61B9B350  12052  1  IP Addresses
0x614246F8  4148  1  AAA Unique Id Hash Table
0x61BA93CC  3688  1  IPAD DIT chunk
0x63B630A4  2544  12  Autoinstall
0x61824BFC  2084  2  CEF: fid GSB
0x62E832EC  2052  1  Reg Function 1
0x62E8A028  1824  24  Autoinstall
0x617DE354  1552  2  CEF: paths
0x6149E638  1552  1  String-DB owne
0x6149F490  1552  1  String-DB entr
0x60191180  846  8  AF entry
0x60191188  1216  8  AF entry
0x617EB5AC  1744  2  CEF: pathl
0x62EAE860  1156  1  Event Manager Table
0x6149E4BC  920  12  NameDB String
0x6176B1F4  884  2  Ether OAM subblock
```

The following is sample output from the `show memory processor fragment` command:

```
Router# show memory processor fragment

Free memory size : 3144348 Number of free blocks: 96

PC  Total  Count  Name
---  ------  ----  -----  
0x669A038  262196  1  TACL FLT
0x62224A8  219188  1  QOS_MODULE_MAIN
0x61648840  131124  1  Init
0x6218DAA4  73780  1  CCSIP_UDP_SOCKET
0x61649288  65588  1  CEF: loadinfo chunk
0x61BF4D8  65588  1  PPTP mgd timer chunk
0x61EE1050  65588  1  eddri_self_event
0x607C13C4  49204  1  Exec
0x605A0D4C  35208  4  Process Stack
0x6059D804  32052  1  TACL hist
0x61631A90  21444  2  CEF: IPv4 Unicast RPF subblock
0x628A5DD8  20432  1  Init
0x6086F858  20052  1  RMI-RO_RU Chun
0x608CF99C  20052  1  Managed Chunk Queue Elements
```

The table below describes the significant fields shown in the display.
Table 126: show memory processor fragment Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>Program counter.</td>
</tr>
<tr>
<td>Total</td>
<td>Total memory allocated by the process (in bytes).</td>
</tr>
<tr>
<td>Count</td>
<td>Number of allocations.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the allocating process.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show memory processor free` command:

```
Router# show memory processor free
Processor memory
Address Bytes Prev Next Ref PrevF NextF Alloc PC what
24 Free list 1
66994680 0000000072 66994618 669946FC 000 0 6698FFC8 60699114 Turbo ACr
6698FFC8 0000000072 6698FF60 66990044 000 66994680 659CF6B0 60699114 Turbo ACr
659CF6B0 0000000024 659CF678 659CF6FC 000 6698FFC8 659CF86C 6078A2CC Init
659CF86C 0000000024 659CF710 659CF8B8 000 659CF6B0 65ADB53C 6078A2CC Init
65ADB53C 0000000024 65ADB504 65ADB588 000 659CF86C 65ADFC38 6078A2CC Init
65ADFC38 0000000024 65ADFC00 65ADFC84 000 65ADB53C 65B6C504 6078A2CC Init
65B6C504 0000000024 65B6C4B8 65B6C550 000 65ADFC38 6593E924 6078A2CC Init
6593E924 0000000028 6593E8B8 6593E974 000 65B6C504 65CCB054 6078A2CC Init
65CCB054 0000000024 65CCB01C 65CCB0A0 000 6593E924 65CCB968 6078A2CC Init
65CCB968 0000000028 65CCBDE8 65CCBDE8 000 65CCB054 65CCB70 6078A2CC Init
65CCB70 0000000024 65CCB38 65CCB6C0 000 65CCB098 65DBB858 6078A2CC Init
65DBB858 0000000024 65DBB20 65DBB84 000 65CCB70 65D0C5F0 6078A2CC Init
65D0C5F0 0000000024 65D0C5B8 65D0C63C 000 65DBB858 65CCFB2F4 6078A2CC Init
65CCFB2F4 0000000024 65CFF2FC 65CFF340 000 65D0C5F0 6608B7B8 6078A2CC Init
6608B7B8 0000000036 6609AFC8 6609B810 000 65CCFB2F4 660A08D4 6078A2CC Init
```

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

Table 127: show memory processor free Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev</td>
<td>Address of the preceding block (should match the address on the preceding row).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of the following block (should match the address on the following row).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of the preceding free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of the following free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the program counter that allocated the block.</td>
</tr>
<tr>
<td>what</td>
<td>Name of the process that owns the block.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show memory processor statistics` command:

```
Router# show memory processor statistics
Head    Total(b)     Used(b)    Free(b)    Lowest(b)    Largest(b)
Processor 6540BBA0  415187836  27216968  387970868  385755044  381633404
         I/O        33554432  6226336    27328096    27328096  27317852
```

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

```
Table 128: show memory processor statistics Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>Hexadecimal address of the head of the memory allocation chain.</td>
</tr>
<tr>
<td>Total(b)</td>
<td>Sum of the used bytes plus free bytes.</td>
</tr>
<tr>
<td>Used(b)</td>
<td>Amount of memory in use (in bytes).</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of memory not in use (in bytes).</td>
</tr>
<tr>
<td>Lowest(b)</td>
<td>Smallest amount of free memory since the last boot (in bytes).</td>
</tr>
<tr>
<td>Largest(b)</td>
<td>Size of the largest available free block (in bytes).</td>
</tr>
</tbody>
</table>
```

**show memory scan**

To monitor the number and type of parity (memory) errors on your system, use the `show memory scan` command in EXEC mode.

```
show memory scan
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(4)XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>This command was implemented in Cisco IOS Release 12.0(7) T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows a result with no memory errors:

```
Router# show memory scan
Memory scan is on.
No parity error has been detected.
```
If errors are detected in the system, the show memory scan command generates an error report. In the following example, memory scan detected a parity error:

```
Router# show memory scan
Memory scan is on.
Total Parity Errors 1.
Address BlockPtr BckSize Disposit Region Timestamp
6115ABCD 60D5D090 9517A4 Scrubed Local 16:57:09 UTC Thu Mar 18
```

The table below describes the fields contained in the error report.

### Table 129: show memory scan Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The byte address where the error occurred.</td>
</tr>
<tr>
<td>BlockPtr</td>
<td>The pointer to the block that contains the error.</td>
</tr>
<tr>
<td>BckSize</td>
<td>The size of the memory block</td>
</tr>
<tr>
<td>Disposit</td>
<td>The action taken in response to the error:</td>
</tr>
<tr>
<td></td>
<td>• BlockInUse--An error was detected in a busy block.</td>
</tr>
<tr>
<td></td>
<td>• InFieldPrev--An error was detected in the previous field of a block header.</td>
</tr>
<tr>
<td></td>
<td>• InHeader--An error was detected in a block header.</td>
</tr>
<tr>
<td></td>
<td>• Linked--A block was linked to a bad list.</td>
</tr>
<tr>
<td></td>
<td>• MScrubed--The same address was “scrubbed” more than once, and the block was linked to a bad list.</td>
</tr>
<tr>
<td></td>
<td>• MultiError--Multiple errors have been found in one block.</td>
</tr>
<tr>
<td></td>
<td>• NoBlkHdr--No block header was found.</td>
</tr>
<tr>
<td></td>
<td>• NotYet--An error was found; no action has been taken at this time.</td>
</tr>
<tr>
<td></td>
<td>• Scrubed--An error was “scrubbed.”</td>
</tr>
<tr>
<td></td>
<td>• SplitLinked--A block was split, and only a small portion was linked to a bad list.</td>
</tr>
<tr>
<td>Region</td>
<td>The memory region in which the error was found:</td>
</tr>
<tr>
<td></td>
<td>• IBSS--image BSS</td>
</tr>
<tr>
<td></td>
<td>• IData--imagedata</td>
</tr>
<tr>
<td></td>
<td>• IText--imagetext</td>
</tr>
<tr>
<td></td>
<td>• local--heap</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The time the error occurred.</td>
</tr>
</tbody>
</table>
show memory statistics history

To display the history of memory consumption, use the `show memory statistics history` command in user EXEC or privileged EXEC mode.

```
show memory statistics history [table]
```

**Syntax Description**

- **table**: (Optional) Summary of memory consumption history.

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show memory statistics history table` command. The field descriptions are self-explanatory.

```
Router# show memory statistics history table
History for Processor memory
Time: 15:48:56.806
Used(b): 422748036 Largest(b): 381064952 Free blocks :291
Maximum memory users for this period
  Process Name   Holding   Num Alloc
    Virtual Exec  26992     37
    TCP Protocols 14460     6
    IP Input      1212      1
Time: 14:42:54.506
Used(b): 422705876 Largest(b): 381064952 Free blocks :296
Maximum memory users for this period
  Process Name   Holding   Num Alloc
    Exec         400012740   24
    Dead         1753456     90
    Pool Manager 212796     257
Time: 13:37:26.918
Used(b): 20700520 Largest(b): 381064952 Free blocks :196
Maximum memory users for this period
  Process Name   Holding   Num Alloc
    Exec         8372      5
Time: 12:39:44.422
Used(b): 20701436 Largest(b): 381064952 Free blocks :193
Time: 11:46:25.135
Used(b): 20701436 Largest(b): 381064952 Free blocks :193
Maximum memory users for this period
  Process Name   Holding   Num Alloc
    CDP Protocol  3752      25
Time: 10:44:24.342
Used(b): 20701400 Largest(b): 381064952 Free blocks :194
Time: 09:38:53.038
Used(b): 20701400 Largest(b): 381064952 Free blocks :194
Time: 08:33:35.154
Used(b): 20701400 Largest(b): 381064952 Free blocks :194
Time: 07:28:05.987
Used(b): 20701400 Largest(b): 381064952 Free blocks :194
```
show memory statistics history

<table>
<thead>
<tr>
<th>Time</th>
<th>Used (b)</th>
<th>Largest (b)</th>
<th>Free blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>06:35:22.878</td>
<td>20701400</td>
<td>381064952</td>
<td>194</td>
</tr>
<tr>
<td>05:42:14.286</td>
<td>20701400</td>
<td>381064952</td>
<td>194</td>
</tr>
<tr>
<td>04:41:53.486</td>
<td>20701400</td>
<td>381064952</td>
<td>194</td>
</tr>
<tr>
<td>03:48:47.891</td>
<td>20701400</td>
<td>381064952</td>
<td>194</td>
</tr>
<tr>
<td>02:46:32.391</td>
<td>20701400</td>
<td>381064952</td>
<td>194</td>
</tr>
<tr>
<td>01:54:27.931</td>
<td>20717804</td>
<td>381064952</td>
<td>189</td>
</tr>
<tr>
<td>01:02:05.535</td>
<td>20717804</td>
<td>381064952</td>
<td>189</td>
</tr>
</tbody>
</table>

Maximum memory users for this period:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Holding</th>
<th>Num Alloc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity MIB API</td>
<td>67784</td>
<td>16</td>
</tr>
<tr>
<td>TTY Background</td>
<td>12928</td>
<td>4</td>
</tr>
<tr>
<td>Exec</td>
<td>7704</td>
<td>3</td>
</tr>
</tbody>
</table>

Time: 00:00:17.936

Maximum memory users for this period:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Holding</th>
<th>Num Alloc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>18653520</td>
<td>6600</td>
</tr>
<tr>
<td>CCPROXY_CT</td>
<td>590068</td>
<td>57</td>
</tr>
<tr>
<td>Proxy Session Applic</td>
<td>275424</td>
<td>21</td>
</tr>
</tbody>
</table>

History for I/O memory:

<table>
<thead>
<tr>
<th>Time</th>
<th>Used (b)</th>
<th>Largest (b)</th>
<th>Free blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:48:56.809</td>
<td>7455520</td>
<td>59370080</td>
<td>164</td>
</tr>
<tr>
<td>14:42:54.508</td>
<td>7458064</td>
<td>59370080</td>
<td>165</td>
</tr>
</tbody>
</table>

Maximum memory users for this period:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Holding</th>
<th>Num Alloc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Manager</td>
<td>141584</td>
<td>257</td>
</tr>
</tbody>
</table>
Maximum memory users for this period

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Holding</th>
<th>Num Alloc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>7296000</td>
<td>214</td>
</tr>
<tr>
<td>Pool Manager</td>
<td>816</td>
<td>3</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>memory statistics history table</code></td>
<td>Changes the memory log time.</td>
</tr>
</tbody>
</table>

**show memory traceback**

To display memory traceback information, use the `show memory traceback` command in privileged EXEC mode.

```
show memory traceback [{id|exclusive|totals}]
```

**Syntax Description**

- **id** *(Optional)* Traceback ID.
- **exclusive** *(Optional)* Displays the memory blocks that have traceback information.
- **totals** *(Optional)* Displays information about memory usage of blocks having tracebacks.

**Command Modes**

Privileged EXEC (#)

**Command History**

- **Release** 15.0(1)M
  - This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

**Usage Guidelines**

Before you can enable the `show memory traceback` command, you must configure the `memory record events` command in global configuration mode.

**Examples**

The following is sample output from the `show memory traceback` command for traceback ID 100:

```
Router# configure terminal
Router(config)# memory record events
Memory event recording already enabled!
Router(config)# exit
Router# show memory traceback 100
Traceback: [100] 0x60630D9Cz 0x60632B50z 0x6063426Cz 0x6063483Cz 0x61AE4910
```

The following is sample output from the `show memory traceback` command using the `exclusive` keyword:

```
Router# configure terminal
Router(config)# memory record events
Memory event recording already enabled!
Router(config)# exit
Router# show memory traceback exclusive
Address Size refcount tid What
```
The table below describes the significant fields shown in the display.

**Table 130: show memory traceback Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Size</td>
<td>Amount of memory, in bytes, used by the task.</td>
</tr>
<tr>
<td>refcount</td>
<td>Reference count for the memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>tid</td>
<td>Task ID.</td>
</tr>
<tr>
<td>What</td>
<td>Name of the process that owns the block or fragment. Specifies if the block is a fragment or coalesced.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory events</td>
<td>Displays recorded memory events.</td>
</tr>
</tbody>
</table>

**show memory transient**

To display statistics about transient memory, use the `show memory transient` command in user EXEC or privileged EXEC mode.

```
show memory transient [{allocating-process |totals}|dead |totals]|fragment |detail]|free |totals]|statistics |history}] |}
```

**Syntax Description**

- `allocating-process` (Optional) Displays allocating memory totals by name.
- `dead | totals` (Optional) Displays memory totals on dead processes.
- `fragment | detail` (Optional) Displays memory statistics for fragmented processes.
- `free | totals` (Optional) Displays statistics on free memory.
- `statistics | history` (Optional) Displays memory pool history statistics on all processes.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show memory transient` command:
Router# show memory transient

<table>
<thead>
<tr>
<th>Address</th>
<th>Bytes</th>
<th>Prev</th>
<th>Next</th>
<th>Ref</th>
<th>PrevF</th>
<th>NextF</th>
<th>Alloc PC</th>
<th>what</th>
</tr>
</thead>
<tbody>
<tr>
<td>81F99C00</td>
<td>0002236408</td>
<td>00000000</td>
<td>821BBC28</td>
<td>000</td>
<td>829C8104</td>
<td>82776FD0</td>
<td>8060B6D0</td>
<td>(coalesc)</td>
</tr>
<tr>
<td>821BBC28</td>
<td>0000020004</td>
<td>81F99C00</td>
<td>821C0A7C</td>
<td>001</td>
<td>--------</td>
<td>--------</td>
<td>8002D5C0</td>
<td>Managed s</td>
</tr>
<tr>
<td>821C0A7C</td>
<td>0000010004</td>
<td>821BBC28</td>
<td>821C31C0</td>
<td>001</td>
<td>--------</td>
<td>--------</td>
<td>811604C0</td>
<td>List Eles</td>
</tr>
<tr>
<td>821C31C0</td>
<td>0000005004</td>
<td>821C0A7C</td>
<td>821C457C</td>
<td>001</td>
<td>--------</td>
<td>--------</td>
<td>81160500</td>
<td>List Heas</td>
</tr>
</tbody>
</table>

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

**Table 131: show memory transient Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Hexadecimal address of the block.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the block (in bytes).</td>
</tr>
<tr>
<td>Prev</td>
<td>Address of the preceding block (should match the address on preceding line).</td>
</tr>
<tr>
<td>Next</td>
<td>Address of the following block (should match the address on following line).</td>
</tr>
<tr>
<td>Ref</td>
<td>Reference count for that memory block, indicating how many different processes are using that block of memory.</td>
</tr>
<tr>
<td>PrevF</td>
<td>Address of the preceding free block (if free).</td>
</tr>
<tr>
<td>NextF</td>
<td>Address of the following free block (if free).</td>
</tr>
<tr>
<td>Alloc PC</td>
<td>Address of the system call that allocated the block.</td>
</tr>
<tr>
<td>what</td>
<td>Name of the process that owns the block, or &quot;(fragment)&quot; if the block is a fragment, or &quot;(coalesced)&quot; if the block was coalesced from adjacent free blocks.</td>
</tr>
</tbody>
</table>

**show microcode**

To display microcode image information available on line cards, use the `show microcode` command in EXEC mode.

**show microcode**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show microcode` command:
Router# show microcode

Microcode bundled in system

<table>
<thead>
<tr>
<th>Type</th>
<th>Version</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP</td>
<td>2.3</td>
<td>11.x</td>
</tr>
<tr>
<td>EIP</td>
<td>1.1</td>
<td>1.x</td>
</tr>
<tr>
<td>TRIP</td>
<td>1.2</td>
<td>1.x</td>
</tr>
<tr>
<td>FIP</td>
<td>1.4</td>
<td>2.x</td>
</tr>
<tr>
<td>HIP</td>
<td>1.1</td>
<td>1.x</td>
</tr>
<tr>
<td>SIP</td>
<td>1.1</td>
<td>1.x</td>
</tr>
<tr>
<td>FSIP</td>
<td>1.1</td>
<td>1.x</td>
</tr>
</tbody>
</table>

In the following example for the Cisco 7200 series router, the output from the `show microcode` command lists the hardware types that support microcode download. For each type, the default microcode image name is displayed. If there is a configured default override, that name also is displayed.

```
router# show microcode
Microcode images for downloadable hardware

<table>
<thead>
<tr>
<th>HW Type</th>
<th>Microcode image names</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecpa</td>
<td>default slot0:xcpa26-0</td>
</tr>
<tr>
<td></td>
<td>configured slot0:xcpa26-2</td>
</tr>
<tr>
<td>pcpa</td>
<td>default slot0:xcpa26-4</td>
</tr>
</tbody>
</table>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>microcode (7000/7500)</td>
<td>Specifies where microcode should be loaded from on Cisco 7500/7000RSP routers.</td>
</tr>
<tr>
<td>microcode (7200)</td>
<td>Configures a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router.</td>
</tr>
</tbody>
</table>

**show mls statistics**

To display the Multilayer Switching (MLS) statistics for the Internet Protocol (IP), Internetwork Packet Exchange (IPX), multicast, Layer 2 protocol, and quality of service (QoS), use the `show mls statistics` command in user EXEC or privileged EXEC mode.

```
show mls statistics [module num]
```

**Syntax Description**

| module num | (Optional) Displays the MLS statistics for a specific module. |

**Command Default**

This command has no default settings.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was changed to include the module num keyword and argument.</td>
</tr>
</tbody>
</table>
ModificationRelease
Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

12.2(17d)SXB1 The output was changed to include total packets switched information.

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(17d)SXB1</td>
<td>The output was changed to include total packets switched information.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The total packets switched performance displayed is the rate calculated as the average rate in a period within the last 30 seconds.

The ingress ACL denied packet count is displayed in the Total packets L3 Switched field and in the Total packets dropped by ACL field.

The RPF failed packet count is displayed in the Total packets L3 Switched field.

If the IP multicast source sends traffic to any multicast group that does not have an (*,G) entry present in the mroutetable, the `show mls statistics` command displays these packets as incrementing in the Total Mcast Packets Switched/Routed field. These packets are dropped in the hardware because there are no receivers for that group and no entry in the mroutetable.

**Examples**

This example shows how to display the MLS statistics for all modules:

```
Router# show mls statistics
Statistics for Earl in Module 2
L2 Forwarding Engine
   Total packets Switched : 20273@ 22552 pps
L3 Forwarding Engine
   Total Packets Bridged : 20273
   Total Packets FIB Switched : 7864
   Total Packets ACL Routed : 0
   Total Packets Netflow Switched : 0
   Total Mcast Packets Switched/Routed : 220598
   Total ip packets with TOS changed : 0
   Total ip packets with COS changed : 0
   Total non ip packets COS changed : 0
   Total packets dropped by ACL : 0
   Total packets dropped by Policing : 705757744
Statistics for Earl in Module 9
L2 Forwarding Engine
   Total packets Switched : 16683@ 1 pps
L3 Forwarding Engine
   Total Packets Bridged : 0
   Total Packets FIB Switched : 0
   Total Packets ACL Routed : 0
   Total Packets Netflow Switched : 0
   Total Mcast Packets Switched/Routed : 0
   Total ip packets with TOS changed : 0
   Total ip packets with COS changed : 0
   Total non ip packets COS changed : 0
   Total packets dropped by ACL : 0
   Total packets dropped by Policing : 277949053
Router#
```

This example shows how to display the MLS statistics for a specific module:
Router# show mls statistics module 1

Statistics for Earl in Module 1

L2 Forwarding Engine
Total packets Switched : 2748166 @ 22332 pps

L3 Forwarding Engine
Total Packets Bridged : 92750 @ 34 pps
Total Packets FIB Switched : 7
Total Packets ACL Routed : 0
Total Packets Netflow Switched : 0
Total Mcast Packets Switched/Routed : 3079200
Total ip packets with TOS changed : 0
Total ip packets with COS changed : 0
Total non ip packets COS changed : 0
Total packets dropped by ACL : 0
Total packets dropped by Policing : 0
Total Unicast RPF failed packets : 0

Errors
MAC/IP length inconsistencies : 0
Short IP packets received : 0
IP header checksum errors : 0
MAC/IPX length inconsistencies : 0
Short IPX packets received : 0

Router
#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mls ascii</td>
<td>display the application-specific integrated circuit (ASIC) version</td>
</tr>
<tr>
<td>show mls df-table</td>
<td>Displays information about the DF table.</td>
</tr>
<tr>
<td>show mls ip</td>
<td>Displays the Multilayer Switching (MLS) IP information.</td>
</tr>
<tr>
<td>show mls ipx</td>
<td>Displays the Multilayer Switching (MLS) IPX information.</td>
</tr>
<tr>
<td>show mls qos</td>
<td>Displays Multilayer Switching (MLS) quality of service (QoS) information</td>
</tr>
<tr>
<td>show mls statistics</td>
<td>Displays the Multilayer Switching (MLS) statistics for the Internet Protocol (IP)</td>
</tr>
</tbody>
</table>

show module

To display the module status and information, use the show module command in user EXEC or privileged EXEC mode.

show module [mod-num|all|provision|version]

Syntax Description

| mod -num | (Optional) Number of the module. |
| all | (Optional) Displays the information for all modules. |
| provision | (Optional) Displays the status about the module provisioning. |
| version | (Optional) Displays the version information. |
This command has no default settings.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In the Mod Sub-Module fields, the `show module` command displays the supervisor engine number but appends the uplink daughter card’s module type and information.

Entering the `show module` command with no arguments is the same as entering the `show module all` command.

**Examples**

This example shows how to display information for all modules on a Cisco 7600 series router that is configured with a Supervisor Engine 720:

```
Router# show module
Mod Ports Card Type Model Serial No.
--- ----- -------------------------- -------------------------- ---
1 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL0843557C
2 48 48-port 10/100/1000 RJ45 EtherModule WS-X6148A-GE-45AF SAL1109HZW9
3 48 48-port 10/100/1000 RJ45 EtherModule WS-X6148A-GE-45AF SAL1114KYZ7
4 48 48 port 10/100 mb RJ45 WS-X6348-RJ-45 SAL0543DGZ1
6 2 Supervisor Engine 720 (Active) WS-SUP720-3B SAL1016KASS
7 48 48-port 10/100 mb RJ45 WS-X6148-45AF SAL08321X1H
8 4 CEF720 4 port 10-Gigabit Ethernet WS-X6704-10GE SAL08528ADQ
9 48 48-port 100FX SFP Ethernet Module WS-X6148-FE-SFP SAD090208MB
Mod MAC addresses Hw Fw Sw Status
--- ----------------------------------- ------ ------------ ------------- ------- -------
1 0012.005c.86e0 to 0012.005c.870f 2.1 12.2(14)S5 12.2(33)SXH Ok
2 0001.005c.86e0 to 0001.005c.870f 2.1 12.2(14)S5 12.2(33)SXH Ok
3 001b.0ce4.9fb0 to 001b.0ce4.9fdf 2.2 8.4(1) 8.7(0.22)SXH Ok
4 0007.4f6c.69f8 to 0007.4f6c.6af7 5.0 5.4(2) 8.7(0.22)SXH Ok
6 0017.9441.44cc to 0017.9441.44cf 5.2 8.4(2) 12.2(33)SXH Ok
7 0011.db0e.c260 to 0011.db0e.c28f 1.1 5.4(2) 8.7(0.22)SXH Ok
8 0002.db99.a43c to 0002.db99.a43f 2.0 12.2(14)x 12.2(33)SXH Ok
9 0030.f273.baf0 to 0030.f273.baf1 3.0 8.4(1) 8.7(0.22)SXH Ok
Mod Sub-Module Model Serial Hw Status
--- ------------------------------- ---
1 Centralized Forwarding Card WS-F6700-CFC SAL08363HL6 2.0 Ok
2 IEEE Voice Daughter Card WS-F6K-48-AF SAL1108HRB1 2.3 Ok
3 IEEE Voice Daughter Card WS-F6K-48-AF SAL1114KV3P 2.3 Ok
4 Inline Power Module WS-F6K-VPWR 1.0 Ok
6 Policy Feature Card 3 WS-F6K-PFC3B SAL1015K00Q 2.3 Ok
6 MSFC3 Daughterboard WS-SUP720 SAL1016KBY3 2.5 Ok
7 IEEE Voice Daughter Card WS-F6K-6E48-AF SAL083111GL 1.1 Ok
8 Centralized Forwarding Card WS-F6700-CFC SAL090204OK 2.0 Ok
Mod Online Diag Status
--- ---
1 Bypass
2 Bypass
3 Bypass
4 Bypass
```
This example shows how to display information for a specific module:

```
Router# show module 2
Mod Ports Card Type Model Serial No.   
--- ----- -------------------------------------- ------------------ -----------
5    2 Supervisor Engine 720 (Active) WS-SUP720-BASE SAD0644030K 
Mod MAC addresses Hw Fw Sw Status
--- ------------------------------------------------- -------------- -------
5 00e0.aabb.cc00 to 00e0.aabb.cc3f 1.0 12.2(2003012 12.2(2003012 Ok
Mod Sub-Module Model Serial Hw Status
--- --------------------------- --------------- --------------- ------- -------
5 Policy Feature Card 3 WS-F6K-PFC3 SAD0644031P 0.302 Ok
5 MSFC3 Daughtercard WS-SUP720 SAD06460172 0.701
Mod Online Diag Status
--- -------------------
5 Not Available
```

This example shows how to display version information:

```
Router# show module version
Mod Port Model Serial # Versions
--- ---- ------------------ ----------- --------------------------------------
2 0 WS-X6182-2PA   
   Hw : 1.0  
   Fw : 12.2(20030125:231135)  
   Sw : 12.2(20030125:231135)
4 16 WS-X6816-GBIC SAD04400CEE Hw : 0.205
   WS-F6K-DFC3A SAD0641029Y Hw : 0.501
   Fw : 12.2(20020828:202911)
   Sw : 12.2(20030125:231135)
6 2 WS-X6K-SUP3-BASE SAD064300GU Hw : 0.705
   Fw : 7.1(0.12-Eng-02)TAM
   Sw : 12.2(20030125:231135)
   Sw1: 8.1(0.45)KIS
   WS-X6K-SUP3-PFC3 SAD064200VR Hw : 0.701
   Fw : 12.2(20021016:001154)
   Sw : 12.2(20030125:231135)
   WS-F6K-PFC3 SAD064300M7 Hw : 0.301
   Fw : 6.3(1)
   Sw : 7.5(0.30)CFW11
```

This example shows how to display module provisioning information:

```
Router# show module provision
Module Provision
  1 dynamic
  2 dynamic
  3 dynamic
  4 dynamic
  5 dynamic
  6 dynamic
  7 dynamic
```
8  dynamic
9  dynamic
10 dynamic
11 dynamic
12 dynamic
13 dynamic
Router#  

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show interfaces</code></td>
<td>Displays the status and statistics for the interfaces in the chassis.</td>
</tr>
<tr>
<td></td>
<td><code>show environment alarm</code></td>
<td>Displays the information about the environmental alarm.</td>
</tr>
<tr>
<td></td>
<td><code>show fm summary</code></td>
<td>Displays a summary of FM Information.</td>
</tr>
<tr>
<td></td>
<td><code>show environment status</code></td>
<td>Displays the information about the operational FRU status.</td>
</tr>
</tbody>
</table>

**show monitor event-trace**

To display event trace messages for Cisco IOS software subsystem components, use the `show monitor event-trace` command in privileged EXEC mode.

```
show monitor event-trace [all-traces] component [all|back hour:minute|clock hour:minute|from-boot seconds|latest|parameters]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>all-traces</th>
<th>(Optional) Displays all event trace messages in memory to the console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>component</td>
<td>(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the <code>monitor event-trace ?</code> command.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all event trace messages currently in memory.</td>
</tr>
<tr>
<td>back mmm</td>
<td>hhh:mm</td>
</tr>
<tr>
<td>clock hh:mm</td>
<td>Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).</td>
</tr>
<tr>
<td>date</td>
<td>(Optional) Day of the month.</td>
</tr>
<tr>
<td>month</td>
<td>(Optional) Displays the month of the year.</td>
</tr>
<tr>
<td>from-boot seconds</td>
<td>Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the <code>show monitor event-trace component from-boot ?</code> command.</td>
</tr>
<tr>
<td>latest</td>
<td>Displays only the event trace messages since the last <code>show monitor event-trace</code> command was entered.</td>
</tr>
</tbody>
</table>
**component**
(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the **monitor event-trace ?** command.

**parameters**
Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

**detail**
(Optional) Displays detailed trace information.

---

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(18)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(8)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S. The <strong>show monitor event-trace cef</strong> command replaced the <strong>show cef events</strong> and <strong>show ip cef events</strong> commands.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE. The <strong>spa</strong> component keyword was added to support online insertion and removal (OIR) event messages for shared port adapters (SPAs). The <strong>bfd</strong> keyword was added for the component argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>Support for the <strong>bfd</strong> keyword was added for Cisco IOS Release 12.4(4)T.</td>
</tr>
<tr>
<td>12.0(31)S</td>
<td>Support for the <strong>bfd</strong> keyword was added for Cisco IOS Release 12.0(31)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.4(9)T</td>
<td>The <strong>cfd</strong> keyword was added as an entry for the component argument to display trace messages relating to crypto fault detection.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>IOS XE Fuji 16.9.1</td>
<td>The subscriber ppp component was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being 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** command will generate a message
indicating that some messages might be lost; however, messages will continue to display on the console. If
the number of lost messages is excessive, the `show monitor event-trace` command will stop displaying
messages.

Use the `bfd` keyword for the `component` argument to display trace messages relating to the BFD feature.
Use the `cfd` keyword for the `component` argument to display trace messages relating to the crypto fault detection
feature. This keyword displays the contents of the error trace buffers in an encryption data path.

**Examples**

**IPC Component Example**

The following is sample output from the `show monitor event-trace component` command for the
interprocess communication (IPC) component. Notice that each trace message is numbered and is
followed by a time stamp (derived from the device uptime). Following the time stamp is the
component-specific message data.

```plaintext
Router# show monitor event-trace ipc
3667: 6840.016:Message type:3 Data=0123456789
3668: 6840.016:Message type:4 Data=0123456789
3669: 6841.016:Message type:5 Data=0123456789
3670: 6841.016:Message type:6 Data=0123456
```

**BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T**

Use the `show monitor event-trace bfd all` command to display logged messages for important BFD
events in the recent past. The following trace messages show BFD session state changes:

```plaintext
Router# show monitor event-trace bfd all
 3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
        create, state Unknown -> Fail
 3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
        (from LC)
 3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
        (from LC)
 3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
        (from LC)
 3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
        create, state Unknown -> Fail
 3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
        (from LC)
 3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
        (from LC)
```

To display trace information for all components configured for event tracing on the networking
device, enter the `show monitor event-trace all-traces` command. In this example, separate output
is provided for each event, and message numbers are interleaved between the events.

```plaintext
Router# show monitor event-trace all-traces
Test1 event trace:
 3667: 6840.016:Message type:3 Data=0123456789
 3669: 6841.016:Message type:4 Data=0123456789
 3671: 6842.016:Message type:5 Data=0123456789
 3673: 6843.016:Message type:6 Data=0123456789
```
**SPA Component Example**

The following is sample output from the `show monitor event-trace component latest` command for the `spa` component:

```
Router# show monitor event-trace spa latest
00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted New state:wait_psm_ready
  spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty New state:remove
  spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete New state:idle
00:02:02.308: subslot 2/1: not present, TSM Event:empty New state:remove
  spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty New state:remove
  spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty New state:remove
  spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete New state:idle
```

**Cisco Express Forwarding Component Examples**

If you select Cisco Express Forwarding as the component for which to display event messages, you can use the following additional arguments and keywords: `show monitor event-trace cef [events | interface | ipv6 | ipv4][all]`.

The following examples show the IPv6 or IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv6 all
00:00:24.612: [Default] *::*/*'00 New FIB table [OK]
```

In the following example, all event trace messages for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all
00:00:18.884: SubSys fib_ios_chain init
00:00:18.884: Inat unknown --> RP
00:00:24.584: SubSys fib init
00:00:24.592: SubSys fib_ios init
00:00:24.592: SubSys fib_ios_if init
00:00:24.596: SubSys ipv4fib init
00:00:24.608: SubSys ipv4fib_ios init
00:00:24.612: SubSys ipv6fib_ios init
00:00:24.620: Flag IPv4 CEF enabled set to yes
```
The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all
00:00:24.624: <empty> (sw 4) Create new
00:00:24.624: <empty> (sw 4) SWIDBlnk FastEthernet0/0(4)
00:00:24.624: Fa0/0 (sw 4) NameSet
00:00:24.624: <empty> (hw 1) Create new
00:00:24.624: <empty> (hw 1) HWIDBlnk FastEthernet0/0(1)
00:00:24.624: Fa0/0 (hw 1) NameSet
00:00:24.624: <empty> (sw 3) Create new
00:00:24.624: <empty> (sw 3) SWIDBlnk FastEthernet0/1(3)
00:00:24.624: Fa0/1 (sw 3) NameSet
00:00:24.624: <empty> (hw 2) Create new
```

Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

The following example shows the IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv4 all
00:00:48.244: [Default] 127.0.0.81/32'01 FIB insert [OK]
```

In the following example, all event trace message for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all
00:00:18.884: SubSys fib_ios_chain init
00:00:18.884: Inst unknown -> RP
00:00:24.584: SubSys fib init
00:00:24.592: SubSys fib_ios init
00:00:24.592: SubSys fib_ios_if init
00:00:24.596: SubSys ipv4fib init
00:00:24.608: SubSys ipv4fib_ios init
00:00:24.620: Flag IPv4 CEF enabled set to yes
00:00:24.620: Flag 0x7BF6B62C set to yes
00:00:24.620: Flag IPv4 CEF switching enabled set to yes
00:00:24.624: GState CEF enabled
00:00:24.628: SubSys ipv4fib_les init
00:00:24.628: SubSys ipv4fib_pas init
00:00:24.632: SubSys ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag IPv4 CEF switching running set to yes
```

The following examples show Cisco Express Forwarding interface events:
Router# show monitor event-trace cef interface all
00:00:24.624: <empty> (sw 4) Create new
00:00:24.624: <empty> (sw 4) SWIDBLnk FastEthernet1/0/0(4)
00:00:24.624: Fa0/0 (sw 4) NameSet
00:00:24.624: <empty> (hw 1) Create new
00:00:24.624: <empty> (hw 1) HWIDBLnk FastEthernet1/0/0(1)
00:00:24.624: Fa0/0 (hw 1) NameSet
00:00:24.624: <empty> (sw 3) Create new
00:00:24.624: <empty> (sw 3) SWIDBLnk FastEthernet1/1/0(3)
00:00:24.624: Fa0/1 (sw 3) NameSet
00:00:24.624: <empty> (hw 2) Create new

CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the show monitor event-trace cfd all command. In this example, events are shown separately, each beginning with a time stamp, followed by data from the error trace buffer. Cisco Technical Assistance Center (TAC) engineers can use this information to diagnose the cause of the errors.

If no packets have been dropped, this command does not display any output.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor event-trace (EXEC)</td>
<td>Controls event trace functions for a specified Cisco IOS software subsystem component.</td>
</tr>
<tr>
<td>monitor event-trace (global)</td>
<td>Configures event tracing for a specified Cisco IOS software subsystem component.</td>
</tr>
<tr>
<td>monitor event-trace dump-traces</td>
<td>Saves trace messages for all event traces currently enabled on the networking device.</td>
</tr>
</tbody>
</table>
show monitor permit list through show process memory

• show monitor permit list through show process memory, on page 752
show monitor permit list through show process memory

show monitor permit-list

To display the permit-list state and interfaces configured, use the `show monitor permit-list` command in user EXEC or privileged EXEC mode.

```
show monitor permit-list
```

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXE</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to display the permit-list state and interfaces configured:

```
Router# show monitor permit-list
SPAN Permit-list :Admin Enabled
Permit-list ports :Gi5/1-4,Gi6/1
Router(config)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor permit-list</td>
<td>Configures a destination port permit list or adds to an existing destination port permit list.</td>
</tr>
</tbody>
</table>

show monitor session

To display information about the ERSPAN, SPAN and RSPAN sessions, use the `show monitor session` command in user EXEC mode.

```
show monitor session [{range session-range|local|remote|all|session}] 
show monitor session [{erspan-destination|erspan-source|egress replication-mode capability|detail}]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>range session-range</code></td>
<td>(Optional) Displays a range of sessions; valid values are from 1 to 66.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>(Optional) Displays only local SPAN sessions.</td>
</tr>
<tr>
<td><code>remote</code></td>
<td>(Optional) Displays both RSPAN source and destination sessions.</td>
</tr>
</tbody>
</table>
show monitor session

(Optional) Displays all sessions.

(Optional) Number of the session; valid values are from 1 to 66.

(Optional) Displays information about the destination ERSPAN sessions only. This keyword is not supported on the Supervisor Engine 2.

(Optional) Displays information about the source ERSPAN sessions only. This keyword is not supported on the Supervisor Engine 2.

(Optional) Displays the operational mode and configured mode of the session and module session capabilities.

(Optional) Displays detailed session information.

This command has no default settings.

User EXEC (>

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support was added for the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>Support was added for the erspan-destination and erspan-source keywords on the Supervisor Engine 720 only.</td>
</tr>
<tr>
<td>12.2(18)SXF</td>
<td>This command was updated as follows:</td>
</tr>
<tr>
<td></td>
<td>• Support was added for the Supervisor Engine 32.</td>
</tr>
<tr>
<td></td>
<td>• ERSPAN is supported in any switch fabric module functionality switching mode.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>The egress replication-mode capability keywords were added.</td>
</tr>
</tbody>
</table>

The erspan-destination and erspan-source keywords are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

In releases prior to Release 12.2(18)SXF, ERSPAN is supported on Catalyst 6500 series switches that are operating in compact switch fabric module functionality switching mode only.

Release 12.2(18)SXF and later releases support ERSPAN in any switch fabric module functionality switching mode.

If the switch fabric module functionality switching mode is set to compact, the output of the show commands display “dcef mode” for fabric-enabled modules with DFC3 installed and display “fabric mode” for other fabric-enabled modules.

If the switch fabric module functionality switching mode is set to truncated, the output of the show commands display “fabric mode” for all fabric-enabled modules.

When entering a range of sessions, use a dash (-) to specify a range and separate multiple entries with a comma (,). Do not enter spaces before or after the comma or the dash.
You can enter multiple ranges by separating the ranges with a comma.

If you enter the `show monitor session` command without specifying a session, the information for all sessions is displayed.

**Examples**

This example shows how to display the saved version of the monitor configuration for a specific session:

```
Router# show monitor session 2
Session 2
--------------
Type : Remote Source Session
Source Ports:
   RX Only: Fa1/1-3
   Dest RSPAN VLAN: 901
Router#
```

This example shows how to display the detailed information from a saved version of the monitor configuration for a specific session:

```
Router# show monitor session 2 detail
Session 2
--------------
Type : Remote Source Session
Source Ports:
   RX Only: Fa1/1-3
   TX Only: None
   Both: None
Source VLANs:
   RX Only: None
   TX Only: None
   Both: None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs: None
Dest RSPAN VLAN: 901
Router#
```

This example shows how to display information about the egress replication mode only:

```
Router# show monitor session egress replication-mode capability
No SPAN configuration is present in the system.
-------------------------------------------------------
Global Egress SPAN Replication Mode Capability:
Slot  Egress Replication Capability
  No       LSPAN  RSPAN  ERSSPAN
-------------------------------------------------------
3  Distributed  Distributed  Distributed
5  Distributed  Distributed  Distributed
Router#
```

This example shows how to display information about the destination ERSpan sessions only:

```
Router# show monitor session erspan-destination
Session 2
--------
Type: ERSpan Destination Session
Status: Admin Disabled
Router#
```
This example shows how to display detailed information about the destination ERSPAN sessions only:

```
Router# show monitor session erspan-destination detail

Session 2
---------
Type : ERSPAN Destination Session
Status : Admin Disabled
Description : -
Source Ports :
  RX Only : None
  TX Only : None
  Both : None
Source VLANs :
  RX Only : None
  TX Only : None
  Both : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs : None
Destination RSPAN VLAN : None
Source IP Address : None
Source IP VRF : None
Source ERSPAN ID : None
Destination IP Address : None
Destination IP VRF : None
Destination ERSPAN ID : None
Origin IP Address : None
IP QOS PREC : 0
IP TTL : 255
```

Router#

This example shows how to display information about the source ERSPAN sessions only:

```
Router# show monitor session erspan-source

Session 1
---------
Type : ERSPAN Source Session
Status : Admin Disabled

Session 3
---------
Type : ERSPAN Source Session
Status : Admin Disabled
```

Router#

This example shows how to display detailed information about the source ERSPAN sessions only:

```
Router# show monitor session erspan-source detail

Session 1
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : -
Source Ports :
  RX Only : None
  TX Only : None
  Both : None
```

Router#
Source VLANs:
  RX Only: None
  TX Only: None
  Both: None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs: None
Destination RSPAN VLAN: None
Source IP Address: None
Source IP VRF: None
Source ERSPAN ID: None
Destination IP Address: None
Destination IP VRF: None
Destination ERSPAN ID: None
Origin IP Address: None
IP QOS PREC: 0
IP TTL: 255
Session 3
---------
Type: ERSpan Source Session
Status: Admin Disabled
Description: -
Source Ports:
  RX Only: None
  TX Only: None
  Both: None
Source VLANs:
  RX Only: None
  TX Only: None
  Both: None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs: None
Destination RSPAN VLAN: None
Source IP Address: None
Source IP VRF: None
Source ERSPAN ID: None
Destination IP Address: None
Destination IP VRF: None
Destination ERSPAN ID: None
Origin IP Address: None
IP QOS PREC: 0
IP TTL: 255
Router#

This example shows how to display the operational mode and configured mode of the session and module session capabilities:

Router# show monitor session egress replication-mode capability
Session 65 Type Local Session
-----------------------------------------------
Operational mode of egress span replication: Centralized
Configured mode of egress span replication: Distributed/Default
Slot Egress Replication Capability
-----------------------------------------------
  1 Centralized
  3 Centralized
  5 Centralized
Router#
show msfc

To display Multilayer Switching Feature Card (MSFC) information, use the `show msfc` command in user EXEC or privileged EXEC mode.

```
show msfc {buffers|eeprom|fault|netint|tlb}
```

**Syntax Description**

- **buffers**: Displays buffer-allocation information.
- **eeprom**: Displays the internal information.
- **fault**: Displays fault information.
- **netint**: Displays network-interrupt information.
- **tlb**: Displays information about the TLB registers.

**Command Default**

This command has no default settings.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

These examples display the `show msfc` command output:

```
Router# show msfc buffers
Reg. set  Min  Max
TX        640   640
ABQ       640   16384
  0       0     40
  1       6715  8192
  2       0     0
  3       0     0
  4       0     0
```
Router# show msfc eeprom
RSFC CPU IDPROM:
IDPROM image:
(FRU is 'Cat6k MSFC 2 daughterboard')
IDPROM image block #0:
  hexadecimal contents of block:
  00: AB AB 01 90 13 22 01 00 00 02 60 03 00 EA 43 69 ...."...
  10: 73 63 6F 00 00 02 60 03 00 00 00 00 00 00 00 00 .sco Systems..
  20: 00 00 57 53 20 4D 33 2D 37 32 33 73 63 6F 00 00 .W-37233-sco
  30: 37 73 74 65 6D 73 00 00 00 00 00 00 00 00 00 00 7-..SAD621006
  40: 37 32 33 73 63 6F 00 00 00 00 00 00 00 00 00 00 7-37233-sco
  50: 37 30 33 33 00 00 00 00 00 00 00 00 00 00 00 00 7-303336
  60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 000000
  70: 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 000000
  80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 000000
  block-signature = 0xABAB, block-version = 1,
  block-length = 144, block-checksum = 4898
  *** common-block ***
  IDPROM capacity (bytes) = 256 IDPROM block-count = 2
  FRU type = (0x6003,234)
  OEM String = 'Cisco Systems'
  Product Number = 'WS-F6K-MSFC2'
  Serial Number = 'SAD06210067'
  Manufacturing Assembly Number = '73-7237-03'
  Manufacturing Assembly Revision = 'A0'
  Hardware Revision = 2.3
  Manufacturing bits = 0x0 Engineering bits = 0x0
  SNMP OID = 9.5.1.3.1.1.2.234
  Power Consumption = -33 centiamperes RMA failure code = 0-0-0-0
  *** end of common block ***
IDPROM image block #1:
  hexadecimal contents of block:
  00: 60 03 01 62 0A C2 00 00 00 00 00 00 00 00 00 00 ....b.........
  10: 00 00 00 00 00 01 00 23 00 08 7C 4A CE 80 00 40 .......|.........
  20: 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 ..........0000
  30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 000000
  40: 14 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 000000
  50: 10 00 4B 3C 41 32 80 80 80 80 80 80 80 80 80 80 X<A2........
  60: 80 80 80 ....
  block-signature = 0x6003, block-version = 1,
  block-length = 98, block-checksum = 2754
  *** linecard specific block ***
  feature-bits = 00000000 00000000
  hardware-changes-bits = 00000000 00000000
  card index = 35
  mac base = 0008.7CA4.CE80
  mac_len = 64
  num_processers = 1
  ep1d_num = 1
  ep1d_versions = 0001 0000 0000 0000 0000 0000 0000 0000 0000 0000 00
  00 0000 0000
  port numbers:
    pair #0: type=14, count=01
    pair #1: type=00, count=00
    pair #2: type=00, count=00
    pair #3: type=00, count=00
    pair #4: type=00, count=00
sensor_thresholds =
  sensor #0: critical = 75 oC, warning = 60 oC
  sensor #1: critical = 65 oC, warning = 50 oC
  sensor #2: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
  sensor #3: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
  sensor #4: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
  sensor #5: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
  sensor #6: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
  sensor #7: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)

*** end of linecard specific block ***

End of IDPROM image

Router# show msfc fault
Reg. set Min Max
TX 640
ABQ 640 16384
0 0 40
1 6715 8192
2 0 0
3 0 0
4 0 0
5 0 0
6 0 0
7 0 0
Threshold = 8192
Vlan Sel Min Max Cnt Rsvd
1016 1 6715 8192 0 0

Router# show msfc netint
Network IO Interrupt Throttling:
  throttle count=0, timer count=0
  active=0, configured=1
  netint usec=3999, netint mask usec=400

Router# show msfc tlb
Mistral revision 3
TLB entries : 37
Virt Address range Phy Address range Attributes
0x01000000:0x0101FFFF 0x01000000:0x01001FFFF CacheMode=2, RW, Valid
0x01002000:0x0103FFFF 0x01002000:0x01003FFFF CacheMode=2, RW, Valid
0x01004000:0x0105FFFF 0x01004000:0x01005FFFF CacheMode=2, RW, Valid
0x01006000:0x0107FFFF 0x01006000:0x01007FFFF CacheMode=2, RW, Valid
0x01008000:0x01087FFF 0x01008000:0x010087FFF CacheMode=2, RW, Valid
0x01008000:0x0108FFFF 0x01008000:0x01008FFFF CacheMode=2, RW, Valid
0x01800000:0x01801FFFFF 0x01800000:0x01801FFFF CacheMode=0, RW, Valid
0x01800000:0x01801FFFF 0x01000000:0x01001FFFF CacheMode=7, RW, Valid
0x01E00000:0x01E1FFFF 0x01E00000:0x01E1FFFF CacheMode=2, RW, Valid
0x01E88000:0x01E881FFFF 0x01E88000:0x01E881FFFF CacheMode=2, RW, Valid
0x01FC0000:0x01FC7FFFFF 0x01FC0000:0x01FC7FFFF CacheMode=2, RO, Valid
0x03000000:0x03001FFFFF 0x03000000:0x03001FFFF CacheMode=2, RW, Valid
0x04000000:0x0407FFFFF 0x04000000:0x04007FFFFF CacheMode=3, RO, Valid
0x04080000:0x040FFFFF 0x04080000:0x040FFFFF CacheMode=3, RO, Valid
0x04100000:0x0417FFFFF 0x04100000:0x0417FFFFF CacheMode=3, RO, Valid
0x04180000:0x0419FFFFF 0x04080000:0x04019FFFFF CacheMode=3, RO, Valid
show pagp

To display port-channel information, use the show pagp command in user EXEC or privileged EXEC mode.

```
show pagp [group-number] {counters|internal|neighbor|pgroup}
```

### Syntax Description

- **group-number** *(Optional) Channel-group number; valid values are a maximum of 64 values from 1 to 282.*
- **counters** Displays the traffic information.
- **internal** Displays the internal information.
- **neighbor** Displays the neighbor information.
- **pgroup** Displays the active port channels.

### Command Default

This command has no default settings.

### Command Modes

User EXEC Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can enter any `show pagp` command to display the active port-channel information. To display the nonactive information, enter the `show pagp` command with a group.

The `port-channel number` values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display information about the PAgP counters:

```
Router# show pagp counters
                  Information       Flush
Port   Sent  Recv   Sent  Recv
--------------------------------------
Channel group: 1
   Fa5/4 2660 2452   0    0
   Fa5/5 2676 2453   0    0
Channel group: 2
   Fa5/6 289  261   0    0
   Fa5/7 290  261   0    0
Channel group: 1023
   Fa5/9  0    0    0    0
Channel group: 1024
   Fa5/8  0    0    0    0
Router#
```

This example shows how to display internal PAgP information:

```
Router# show pagp 1 internal
Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.  
       A - Device is in Auto mode.  P - Device learns on physical port.
Timers: H - Hello timer is running.  Q - Quit timer is running.  
        S - Switching timer is running.  I - Interface timer is running.
Channel group 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Hello Interval</th>
<th>Partner Priority</th>
<th>PAgP Learning Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/4</td>
<td>SC</td>
<td>U6/S7</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
</tr>
<tr>
<td>Fa5/5</td>
<td>SC</td>
<td>U6/S7</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
</tr>
</tbody>
</table>

Router#
```

This example shows how to display PAgP-neighbor information for all neighbors:

```
Router# show pagp neighbor
Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.  
       A - Device is in Auto mode.  P - Device learns on physical port.  
       Partner learns on physical port.
Channel group 1 neighbors

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Device ID</th>
<th>Port Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/4</td>
<td>JAB031301</td>
<td>0050.0f10.230c</td>
<td>2/45</td>
<td>2s</td>
<td>SAC</td>
</tr>
<tr>
<td>Fa5/5</td>
<td>JAB031301</td>
<td>0050.0f10.230c</td>
<td>2/46</td>
<td>27s</td>
<td>SAC</td>
</tr>
</tbody>
</table>

Channel group 2 neighbors
```

Cisco IOS Configuration Fundamentals Command Reference 761
**show parser dump**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>pagp learn-method</td>
<td>Learns the input interface of the incoming packets.</td>
</tr>
<tr>
<td></td>
<td>pagp port-priority</td>
<td>Selects a port in hot standby mode.</td>
</tr>
</tbody>
</table>

**Note**

Effective with Cisco IOS Release 15.0(1)M, the `show parser dump` command is not available in Cisco IOS software.

To display the command-line interface (CLI) syntax options for all command modes or for a specified command mode, use the `show parser dump` command in user EXEC or privileged EXEC mode.

```
show parser dump [command-mode|all] [privilege-level level] [extend] [breakage]
```

**Syntax Description**

- **command-mode**
  - A keyword indicating the command mode. The output will include the syntax for commands only in the specified command mode. The list of command mode keywords will vary depending on your software image. Use the `show parser dump ?` command to display the list of command mode keyword options. For further assistance in determining the proper command mode, see the “Cisco IOS Command Modes” Release 12.2 document, available on Cisco.com.

- **all**
  - Indicates that all commands in all modes should be displayed in the output.
  - **Caution** This keyword generates a very large amount of output, which may exceed your system or buffer memory.

- **privilege-level level**
  - (Optional) Lists CLI commands only with the privilege level specified in the `level` argument.

- **extend**
  - (Optional) Enables the extended display mode. The extended parser display shows the keyword and argument descriptions typically shown with the command-line help (`?` command).
  - **Note** This keyword can produce a large amount of output.
**Usage Guidelines**

This command was developed to allow the exploration of the CLI command syntax without requiring the user to actually enter a specific mode and use the `?` command-line help.

Use caution when entering this command with the **all** keyword. A large amount of output can be generated by this command, which may easily exceed buffer or system memory on smaller platforms. Also, some configuration modes have hundreds of valid commands. For large dumps, use of the redirection to a file using the `| redirect URL` syntax at the end of the command is highly recommended. (See the documentation for the `show command redirect` command for more information on using this command extension.)

Output for this command will show the syntax options for all commands available in the specified mode. The number preceding the command shows the privilege level associated with that command. For example, the line

```
15 type dhcp
```

indicates that the **type dhcp** command has a privilege level of 15 assigned to it. For information about privilege levels, see the “Configuring Passwords and Privileges” chapter in the *Cisco IOS Security Configuration Guide*.

Any given command-line string should indicate the full syntax needed to make the command complete and valid. In other words, the command-line string ends where the carriage return (Enter) could be entered, as indicated in command-line help by the `<cr>` syntax. You will typically see multiple forms of a command, each showing a valid syntax combination. For example, each of the following syntax combinations, as seen in the output of the `show parser dump rtr | include dhcp` command, is a valid command:

```
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> circuit-id <string>
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> remote-id <string>
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> subnet-mask <ipmask>
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82>
type dhcp dest-ipaddr <address> source-ipaddr <address>
type dhcp
```

**breakage** *(Optional) Enables detection of potential parser chain syntax breakage. This keyword is intended for internal use.*
Use of the `show` command extensions `| begin`, `| include`, and `| exclude` is recommended for this command because these extensions allow you to filter the output to display only the commands you are interested in. The redirection extensions `| redirect`, `| append`, and `| tee` allow you to redirect the output of this command to local or remote storage as a file.

As with most `show` commands, you can typically exit from the `--More--` prompt back to EXEC mode using `Ctrl-Z`. For some connections, `Ctrl-Shift-6` (`Ctrl^`) or `Ctrl-Shift-6-X` should be used instead.

### Examples

The following example shows a typical list of command mode keywords. The fields are self-explanatory.

```
Router# `show parser dump` ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-attr-list</td>
<td>AAA attribute list config mode</td>
</tr>
<tr>
<td>aaa-user</td>
<td>AAA user definition</td>
</tr>
<tr>
<td>accept-dialin</td>
<td>VPDN group accept dialin configuration mode</td>
</tr>
<tr>
<td>accept-dialout</td>
<td>VPDN group accept dialout configuration mode</td>
</tr>
<tr>
<td>acct_ml_list</td>
<td>AAA accounting methodlist definitions</td>
</tr>
<tr>
<td>address-family</td>
<td>Address Family configuration mode</td>
</tr>
<tr>
<td>acl</td>
<td>Access Control List</td>
</tr>
<tr>
<td>alps-ascu</td>
<td>ALPS ASCU configuration mode</td>
</tr>
<tr>
<td>alps-circuit</td>
<td>ALPS circuit configuration mode</td>
</tr>
<tr>
<td>appfw-application-aim</td>
<td>Appfw for AIM Configuration Mode</td>
</tr>
<tr>
<td>appfw-application-msnmsgr</td>
<td>Appfw for MSN Messenger Configuration Mode</td>
</tr>
<tr>
<td>appfw-application-ymsgr</td>
<td>Appfw for Yahoo! Messenger Configuration Mode</td>
</tr>
<tr>
<td>appfw-policy</td>
<td>Application FW Policy Configuration Mode</td>
</tr>
<tr>
<td>application-http</td>
<td>Appfw for HTTP Configuration Mode</td>
</tr>
<tr>
<td>archive</td>
<td>Archive the router configuration mode</td>
</tr>
<tr>
<td>atalk-test</td>
<td>Appletalk test mode</td>
</tr>
<tr>
<td>atm-bm-config</td>
<td>ATM bundle member configuration mode</td>
</tr>
<tr>
<td>atm-bundle-config</td>
<td>ATM bundle configuration mode</td>
</tr>
<tr>
<td>atm-l2trans-pvc-config</td>
<td>ATM L2transport PVC configuration mode</td>
</tr>
<tr>
<td>atm-l2trans-pvp-config</td>
<td>ATM L2transport PVP configuration mode</td>
</tr>
<tr>
<td>atm-pvc-range-config</td>
<td>ATM PVC Range configuration mode</td>
</tr>
<tr>
<td>atm-range-pvc-config</td>
<td>ATM PVC in Range configuration mode</td>
</tr>
<tr>
<td>atm-svc-bm-config</td>
<td>ATM SVC bundle member configuration mode</td>
</tr>
<tr>
<td>atm-svc-bundle-config</td>
<td>ATM SVC bundle configuration mode</td>
</tr>
<tr>
<td>atm-vc-config</td>
<td>ATM virtual circuit configuration mode</td>
</tr>
<tr>
<td>atmSig_e164_table_mode</td>
<td>ATM SIG E164 Table</td>
</tr>
<tr>
<td>auto-ip-sla-mpls</td>
<td>Auto IP SLA MPLS LSP Monitor configs</td>
</tr>
<tr>
<td>auto-ip-sla-mps-ld-params</td>
<td>Auto IP SLA MPLS LPD params config</td>
</tr>
<tr>
<td>auto-ip-sla-mps-params</td>
<td>Auto IP SLA MPLS LSP Monitor Params configs</td>
</tr>
<tr>
<td>banner</td>
<td>Banner Input mode</td>
</tr>
<tr>
<td>bba-group</td>
<td>BBA Group configuration mode</td>
</tr>
<tr>
<td>boomerang</td>
<td>Boomerang configuration mode</td>
</tr>
<tr>
<td>bsm-cfg</td>
<td>BSM config definition</td>
</tr>
<tr>
<td>bulkstat-objlist</td>
<td>Bulk-stat Object list configuration mode</td>
</tr>
<tr>
<td>bulkstat-schemodef</td>
<td>Bulk-stat schema configuration mode</td>
</tr>
<tr>
<td>bulkstat-transfer</td>
<td>Bulk Stat configuration mode</td>
</tr>
<tr>
<td>cascustom</td>
<td>Cas custom configuration mode</td>
</tr>
<tr>
<td>call-filter-matchlist</td>
<td>Call Filter matchlist configuration mode</td>
</tr>
<tr>
<td>call-home</td>
<td>call-home config mode</td>
</tr>
<tr>
<td>call-home-profile</td>
<td>call-home profile config mode</td>
</tr>
<tr>
<td>call-router</td>
<td>AnnexG configuration mode</td>
</tr>
<tr>
<td>cascustom</td>
<td>Cas custom configuration mode</td>
</tr>
<tr>
<td>cause-code-list</td>
<td>Voice Cause Code List configuration mode</td>
</tr>
<tr>
<td>cfg-path</td>
<td>IP Host backup configuration mode</td>
</tr>
<tr>
<td>cfg-pt-ruleset</td>
<td>Protocol Translation ruleset configuration mode</td>
</tr>
<tr>
<td>cip-vadp</td>
<td>Virtual Adapter configuration mode</td>
</tr>
<tr>
<td>cip-vlan</td>
<td>Virtual Lan configuration mode</td>
</tr>
</tbody>
</table>

*Cisco IOS Configuration Fundamentals Command Reference*
show parser dump
gw Webvpn virtual gateway configuration
gw-accounting-aaa Gateway accounting aaa configuration mode
gw-accounting-file Gateway accounting file configuration mode
hostlist Host list configuration mode
identity-policy-mode Identity policy configuration mode
identity-profile-mode Identity profile configuration mode
interface Interface configuration mode
interface range Interface range configuration mode
interface-dlci Frame Relay dci configuration mode
ip-explicit-path IP explicit path configuration mode
ip sla IP SLAs entry configuration
ip sla-am-grp IP SLAs auto group config
ip sla-am-grp-auto IP SLAs auto group dest-auto config
ip sla-am-schedule IP SLAs auto schedule config
ip sla-dhcp IP SLAs dhcp configuration
ip sla-dns IP SLAs dns configuration
ip sla-echo IP SLAs echo configuration
ip sla-ethernet-echo IP SLAs Ethernet Echo configuration
ip sla-ethernet-jitter IP SLAs Ethernet Jitter configuration
ip sla-ethernet-monitor IP SLAs Ethernet configs
ip sla-ethernet-monitor-params IP SLAs Ethernet Params configs
ip sla-frameRelay IP SLAs FrameRelay configuration
ip sla-ftp IP SLAs ftp configuration
ip sla-http IP SLAs http configuration
ip sla-icmp-ech-params IP SLAs icmpEcho Parameters
ip sla-icmp-jtr-params IP SLAs icmpJitter Parameters
ip sla-icmpjitter IP SLAs icmpjitter configuration
ip sla-jitter IP SLAs jitter configuration
ip sla-pathEcho IP SLAs pathEcho configuration
ip sla-pathJitter IP SLAs pathJitter configuration
ip sla-tcp-conn-params IP SLAs tcpConnect Parameters
ip sla-tcpConnect IP SLAs tcpConnect configuration
ip sla-tplt-dest IP SLAs auto destination submode
ip sla-tplt-icmp-ech IP SLAs auto template icmpEcho
ip sla-tplt-icmp-jtr IP SLAs auto template icmpJitter
ip sla-tplt-tcp-conn IP SLAs auto template tcpConnect
ip sla-tplt-udp-ech IP SLAs auto template udpEcho
ip sla-tplt-udp-jtr IP SLAs auto template udpJitter
ip sla-udp-ech-params IP SLAs udpEcho Parameters
ip sla-udp-jtr-params IP SLAs udpJitter Parameters
ip sla-udpEcho IP SLAs udpEcho configuration
ip sla-volp IP SLAs volp configuration
ip sla-volp-rtp IP SLAs rtp configuration
ip-vrf Configure IP VRF parameters
ipc-zone-assoc-protocol-sctp ip protocol sctp mode
ipczone IPC Zone config mode
ipczone-assoc IPC Association config mode
ipenacl IP named extended access-list configuration mode
iphc-profile-mode IPHC Profile configuration mode
ipmobile-test IP Mobility test mode
ipnat-pool IP NAT pool configuration mode
ipnat-portmap IP NAT portmap configuration mode
ipnat-sbc IP NAT SIP-SBC config mode
ipnat-sbc-vrf IP NAT SIP-SBC vrf config mode
ipnat-snat IP SNAT configuration mode
ipnat-snat-backup IP SNAT Backup configuration mode
ipnat-snat-primary IP SNAT Primary configuration mode
ipnat-snat-redundancy IP SNAT Redundancy configuration mode
ips-seap-rules IPS event action rules configuration mode
ips-sigdef-sig IPS signature number name configuration mode
ipscaction IPS Category name configuration mode
ipsnacl IP named simple access-list configuration mode
ipssigau IPS Auto Update configuration mode
ipssigcat IPS signature category configuration mode
telephony-service-group  Telephony service group configuration mode
telephony-service-video  Telephony service video configuration mode
template  Template configuration mode
template peer-policy  peer-policy configuration mode
template peer-session  peer-session configuration mode
test_cpu  config-owner-test_cpu
test_mem  config-owner-test_mem
tidp-group  TIDP Group configuration mode
tidp-keyset  TIDP key-set configuration mode
tn3270s-dlur  tn3270 server DLUR configuration mode
tn3270s-dlur-pu  tn3270 server DLUR PU configuration mode
tn3270s-dlur-sap  tn3270 server DLUR SAP configuration mode
tn3270s-listen-point  tn3270 server Listen-Point configuration mode
tn3270s-listen-point-pu  tn3270 server Listen-Point PU configuration mode	n3270s-pu  tn3270 server PU configuration mode	n3270s-resp-time  tn3270 server response time client group configuration mode	n3270s-security  tn3270 server Security Configuration mode	n3270s-security-time  tn3270 server Security Time Configuration mode
t3270s-security-profile  tn3270 server Security Profile Configuration mode
tn3270s-svr  tn3270 server configuration mode
top-talkers  Netflow top talkers config mode
tracking-config  Tracking configuration mode
trange  time-range configuration mode
translation-profile  Voice Translation Profile configuration mode
translation-rule  Translation Rule configuration mode
trunk-group  Trunk group configuration mode
vc-class  VC class configuration mode
vc-group  VC group configuration mode
view  View configuration mode
vlan  VLAN database editing buffer
vm-integration  Voicemail integration configuration mode
voice-cause-code  Voice Cause Code configuration mode
voice-gateway  voice gateway configuration mode
voice-mlpp  voice mlpp configuration mode
voice-service  Voice service configuration mode
voice-service-h323  Voice service h323 configuration mode
voice-service-session  Voice service session configuration mode
voice-service-sip  Voice service sip configuration mode
voice-service-stun  Voice service stun configuration mode
voice-uri-class  Voice URI Class configuration mode
voicecl- cptone  Voice Class CPTone configuration mode
voicecl- cptone-dt  CPTone dualtone configuration mode
voicecl- dt-detect  Voice Class Dualtone Detect configuration mode
voiceclass  Voice Class configuration mode
voicednismaps  Dnis Map Configuration
voiceport  Voice configuration mode
voipdialpeer  Dial Peer configuration mode
voipdpcor  Dial Peer Class of Restriction configuration mode
voipdpcorlist  Dial Peer Class of Restriction List configuration mode
vpdn-group  VPDN group configuration mode
vpdn-template  VPDN template configuration mode
vrf  Configure VRF parameters
webvpn  Webvpn virtual context configuration
webvpn-acl  Webvpn ACL configuration
webvpn-cifs-url  Webvpn CIFS URL list configuration
webvpn-group-policy  Webvpn group policy configuration
webvpn-nbnslist  Webvpn VN ctxt NBNS list configuration
webvpn-port-fwd  Webvpn port-forward list configuration
webvpn-ssoserver  SSO Server configuration
webvpn-time-range  Webvpn time range configuration
webvpn-url  Webvpn URL list configuration
webvpn-url-rewrite  Webvpn url-rewrite list configuration
x25-profile  X.25 profile configuration mode
xconnect-conn-config  Xconnect connect configuration submode
xconnect-dlci-config  Xconnect FR DLCI configuration submode
In the following example, only commands in RTR configuration mode are shown:

Router# show parser dump rtr

Mode Name : rtr
  15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535> control enable
  15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535> control disable
  15 type tcpConnect dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535> control enable
  15 type tcpConnect dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535> control disable
  15 type jitter dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535>
  15 type jitter dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535>
  15 type ftp operation get url <string> source-ipaddr <address> mode active
  15 type ftp operation get url <string> source-ipaddr <address> mode passive
  15 type http operation get url <string> name-server <address> version <string> source-ipaddr <address> source-port <1-65535> cache
  15 type http operation get url <string> name-server <address> version <string> source-ipaddr <address> source-port <1-65535> cache
  15 type http operation get url <string> name-server <address> version <string> source-ipaddr <address> source-port <1-65535> cache
  15 type http operation get url <string> name-server <address> version <string> source-ipaddr <address> source-port <1-65535> cache
  15 type http operation get url <string> name-server <address> version <string> source-ipaddr <address> source-port <1-65535> cache
  15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> circuit-id <string>
  15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> circuit-id <string>
  15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> subnet-mask <ipmask>
  15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> subnet-mask <ipmask>
In the following example, only those commands in RTR configuration mode containing the keyword `dhcp` are shown:

Router# show parser dump rtr | include dhcp

The following example shows how the `extend` keyword displays the syntax descriptions that match those shown using the `?` command-line help:

Router# show parser dump rtr extend

Mode Name :rtr
15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address> source-port <1-65535> control enable
type : Type of entry
udpEcho : UDP Echo Operation
dest-ipaddr : Destination address
<address> : IP address or hostname
dest-port : Destination Port
<1-65535> : Port Number
source-ipaddr : Source address
<address> : IP address or hostname
source-port : Source Port
<1-65535> : Port Number
control : Enable or disable control packets
enable : Enable control packets exchange (default)
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# rtr 1

Router(config-rtr)# type udpEcho ?

dest-ipaddr  Destination address

Router(config-rtr)# type udpEcho dest-ipaddr ?

Hostname or A.B.C.D IP address or hostname

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME ?

dest-port  Destination Port

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME dest-port ?

<1-65535>  Port Number

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME dest-port 1 ?

control  Enable or disable control packets
source-ipaddr  Source address
source-port  Source Port
<cr>

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME dest-port 1 control ?

disable  Disable control packets exchange
enable   Enable control packets exchange (default)

In the following example, show parser dump output is redirected to a file on a remote TFTP server:

show parser dump exec extend | redirect tftp://209.165.200.225/userdirectory/123-exec-commands.txt

In the following example, the show parser dump command is not available in Cisco IOS software because this command was removed in Cisco IOS 15.0(1)M:

Router# show parser dump all
Command accepted, but obsolete, parser dumper has been deprecated

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show append</td>
<td>Redirects and adds the output of any show command to an existing file.</td>
</tr>
<tr>
<td></td>
<td>show begin</td>
<td>Filters the output of any show command to display the output from the first instance of a specified string.</td>
</tr>
<tr>
<td></td>
<td>show exclude</td>
<td>Filters show command output so that it excludes lines that contain a particular regular expression.</td>
</tr>
<tr>
<td></td>
<td>show include</td>
<td>Filters show command output so that only lines that containing the specified string are displayed.</td>
</tr>
<tr>
<td></td>
<td>show redirect</td>
<td>Redirects the output of any show command to a file.</td>
</tr>
<tr>
<td></td>
<td>show tee</td>
<td>Copies the output of any show command to a file while displaying it on the terminal.</td>
</tr>
</tbody>
</table>
show parser macro

To display the smart port macros, use the **show parser macro** command in privileged EXEC mode.

```
show parser macro [{name macro-name|brief|description [interface interface]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name macro-name</td>
<td>(Optional) Displays a specific macro.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays the configured macro names.</td>
</tr>
<tr>
<td>description</td>
<td>(Optional) Displays the macro description for all interfaces.</td>
</tr>
<tr>
<td>interface interface</td>
<td>(Optional) Displays the macro description for the specified interface.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the macro description:

```
Router# show parser macro description

Interface   Macro Description
-----------------------------
Fa1/2        desktop-config
```

The following example shows how to display the contents of the cisco-router smart port macro:

```
Router# show parser macro name cisco-router
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Do not apply to EtherChannel/Port Group
# Access Uplink to Distribution
  switchport
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
  switchport trunk native vlan $NVID
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
  switchport trunk allowed vlan VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
# Configure qos to trust this interface
  auto qos voip trust
  mls qos trust dscp
# Ensure fast access to the network when enabling the interface.
```
# Ensure that switch devices cannot become active on the interface.
spanning-tree portfast
spanning-tree bpduguard enable

The following example shows how to list the Cisco-provided smart port macros:

Router# show parser macro brief | include default

default global : cisco-global
default interface: cisco-desktop
default interface: cisco-phone
default interface: cisco-switch
default interface: cisco-router

## show parser statistics

To display statistics about the last configuration file parsed and the status of the Parser Cache feature, use the `show parser statistics` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show parser statistics` command displays two sets of data:

- The number of commands in the configuration file that was last copied into the running configuration, and the time it took for the system to parse them (a configuration file can be loaded into the running configuration at system startup, or by issuing commands such as the `copy source running-config` command).

- The status of the Parser Cache feature (enabled or disabled) and the number of command matches (indicated by hits/misses) since the system was started or since the parser cache was cleared.

The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.

**Examples**

The following example shows sample output from the `show parser statistics` command:
show parser statistics

Router# show parser statistics
Last configuration file parsed: Number of Commands: 1484, Time: 1272 ms
Parser cache: disabled, 0 hits, 2 misses

In this example, the Parser Cache feature is disabled, but shows the hit/miss statistics for the two commands issued while the parser cache was last enabled.

The table below describes the key output fields.

### Table 132: show parser statistics Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last configuration file parsed:</td>
<td>Displays statistics on the last configuration file copied into the running configuration (at startup or using the <code>copy</code> command).</td>
</tr>
<tr>
<td>Number of commands:</td>
<td>The number of command lines in the last configuration file parsed.</td>
</tr>
<tr>
<td>Time:</td>
<td>Time (in milliseconds) taken for the system to load the last configuration file.</td>
</tr>
<tr>
<td>Parser cache:</td>
<td>Displays whether the Parser Cache feature is enabled or disabled, and the hit/miss statistics related to the feature. Statistics are stored since the initialization of the system, or since the last time the parser cache was cleared.</td>
</tr>
<tr>
<td>hits</td>
<td>Number of commands the parser cache was able to parse more efficiently by matching them to similar commands executed previously.</td>
</tr>
<tr>
<td>misses</td>
<td>Number of commands the parser cache was unable to match to previously executed commands. The performance enhancement provided by the Parser Cache feature cannot be applied to unmatched commands.</td>
</tr>
</tbody>
</table>

In the following example the `show parser statistics` command is used to compare the parse time of a large configuration file with the Parser Cache feature disabled and enabled. In this example, a configuration file with 1484 access list commands is loaded into the running configuration.

Router# configure terminal
! parser cache is disabled
Router(config)# no parser cache
! configuration file is loaded into the running configuration
Router# copy slot0:acl_list running-config
.
.
.
Router# show parser statistics
Last configuration file parsed: Number of Commands: 1484, Time: 1272 ms
Parser cache: disabled, 0 hits, 2 misses

! the parser cache is reenabled
Router(config)# parser cache
! configuration file is loaded into the running configuration
Router# copy slot0:acl_list running-config
.
.
.
Router# show parser statistics
Last configuration file parsed: Number of Commands: 1484, Time: 820 ms
Parser cache: enabled, 1460 hits, 26 misses
These results show an improvement to the load time for the same configuration file from 1272 milliseconds (ms) to 820 ms when the Parser Cache feature was enabled. As indicated in the “hits” field of the `show` command output, 1460 commands were able to be parsed more efficiently by the parser cache.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear parser cache</td>
<td>Clears the parse cache entries and hit/miss statistics stored for the Parser Cache feature.</td>
<td></td>
</tr>
<tr>
<td>parser cache</td>
<td>Enables or disables the Parser Cache feature.</td>
<td></td>
</tr>
</tbody>
</table>

**show pci**

To display information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 7200 series routers, use the `show pci` command in EXEC mode.

```
show pci {hardware|bridge [register]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hardware</td>
<td>Displays PCI hardware registers.</td>
<td></td>
</tr>
<tr>
<td>bridge</td>
<td>Displays PCI bridge registers.</td>
<td></td>
</tr>
<tr>
<td>register</td>
<td>(Optional) Number of a specific bridge register in the range from 0 to 7. If not specified, this command displays information about all registers.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command is generally useful for diagnostic tasks performed by technical support only.

**Note**

The `show pci hardware` EXEC command displays a substantial amount of information.

**Examples**

The following is sample output for the PCI bridge register 1 on a Cisco 7200 series router:

```
Router# show pci bridge 1
Bridge 4, Port Adaptor 1, Handle=1
DEC21050 bridge chip, config=0x0
(0x00): cfid = 0x00011011
(0x04): cfcs = 0x02800147
(0x08): cfccid = 0x06040002
(0x0C): cfpmlt = 0x00070007
(0x18): cfsmlt = 0x18050004
```
The following is partial sample output for the PCI hardware register, which also includes information on all the PCI bridge registers on a Cisco 7200 series router:

```
Router# show pci hardware
GT64010 External PCI Configuration registers:
Vendor / Device ID : 0xAB114601 (b/s 0x014611AB)
Status / Command : 0x17018002 (b/s 0x02800117)
Class / Revision : 0x00000006 (b/s 0x06000000)
Latency : 0x0F000000 (b/s 0x0000000F)
RAS[1:0] Base : 0x00000000 (b/s 0x00000000)
RAS[3:2] Base : 0x00000001 (b/s 0x01000000)
CS[2:0] Base : 0x00000000 (b/s 0x00000000)
CS[3] Base : 0x00000000 (b/s 0x00000000)
Mem Map Base : 0x00000114 (b/s 0x11400000)
IO Map Base : 0x01000014 (b/s 0x14000000)
Int Pin / Line : 0x00010000 (b/s 0x00000100)
Bridge 0, Downstream MB0 to MB1, Handle=0
DEC21050 bridge chip, config=0x0
(0x00): cfid = 0x00011011
(0x04): cfcs = 0x02800143
(0x08): cfccid = 0x06040002
(0x0C): cpfmlt = 0x00001180
(0x18): cfsmlt = 0x18000100
(0x1C): cfsis = 0x028009050
(0x20): cfmla = 0x04AF04880
(0x24): cpfmla = 0x04BF04B00
(0x3C): cfbc = 0x00000000
(0x40): cfseed = 0x00100000
(0x44): cfstwt = 0x00008020
```

display information about the Host-PCI bridge, use the **show pci hardware** command in EXEC mode.

**show pci hardware**

To display information about the Host-PCI bridge, use the **show pci hardware** command in EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command is generally useful for diagnostic tasks performed by technical support only:
Router# show pci hardware
hardware PCI hardware registers
Each device on the PCI bus is assigned a PCI device number. For the
C2600, device numbers are as follows:

<table>
<thead>
<tr>
<th>Device</th>
<th>Device number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>First LAN device</td>
</tr>
<tr>
<td>1</td>
<td>Second LAN device</td>
</tr>
<tr>
<td>2</td>
<td>AIM device (if present)</td>
</tr>
<tr>
<td>3</td>
<td>Not presently used</td>
</tr>
<tr>
<td>4</td>
<td>Port module - first PCI device</td>
</tr>
<tr>
<td>5</td>
<td>Port module - second PCI device</td>
</tr>
<tr>
<td>6</td>
<td>Port module - third PCI device</td>
</tr>
<tr>
<td>7</td>
<td>Port module - fourth PCI device</td>
</tr>
<tr>
<td>8-14</td>
<td>Not presently used</td>
</tr>
<tr>
<td>15</td>
<td>Xilinx PCI bridge</td>
</tr>
</tbody>
</table>

**Examples**

The following is partial sample output for the PCI hardware register, which also includes information on all the PCI bridge registers.

router# show pci hardware
XILINX Host-PCI Bridge Registers:
Vendor / Device ID: 0x401310EE
Status / Command: 0x040001C6
PCI Slave Base Reg 0: 0x00000000
PCI Slave Base Reg 1: 0x04000000

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

**Table 133: show pci hardware Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device/Vendor ID</td>
<td>Identifies the PCI vendor and device. The value 0x401310EE identifies the device as the Xilinx-based Host-PCI bridge for the Cisco 2600 router.</td>
</tr>
<tr>
<td>Status/Command</td>
<td>Provides status of the Host-PCI bridge. Refer to the PCI Specification for more information.</td>
</tr>
<tr>
<td>PCI Slave Base Reg 0</td>
<td>The base address of PCI Target Region 0 for the Host-PCI bridge. This region is used for Big-Endian transfers between PCI devices and memory.</td>
</tr>
<tr>
<td>PCI Slave Base Reg 1</td>
<td>The base address of PCI Target Region 1 for the Host-PCI bridge. This region is used for Little-Endian transfers between PCI devices and memory.</td>
</tr>
</tbody>
</table>

**show perf-meas**

To display the performance measurement of the router, use the `show perf-meas` command in user EXEC or privileged EXEC mode.

```
show perf-meas [{report-types|all}]
```
**Syntax Description**

<table>
<thead>
<tr>
<th>report-types</th>
<th>(optional) Reports type. The values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2t-to-hdlc - Display 2t-to-hdlc report 2t-to-modem Display 2t-to-modem report</td>
<td></td>
</tr>
<tr>
<td>• all - Display all reports</td>
<td></td>
</tr>
<tr>
<td>• fe-to-hdlc - Displays fe-to-hdlc report</td>
<td></td>
</tr>
<tr>
<td>• fe-to-modem - Displays fe-to-modem report</td>
<td></td>
</tr>
<tr>
<td>• hdlc-to-2t - Display hdlc-to-2t report</td>
<td></td>
</tr>
<tr>
<td>• hdlc-to-fe - Display hdlc-to-fe report</td>
<td></td>
</tr>
<tr>
<td>• modem-to-2t - Display modem-to-2t report</td>
<td></td>
</tr>
<tr>
<td>• modem-to-fe - Displays modem-to-fe report</td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show perf-meas` command to display the performance measurement of the router.

**Examples**

The following is sample output from the `show perf-meas` command. The field descriptions are self-explanatory.

```
Router# show perf-meas
****** PERFORMANCE MEASUREMENT ******
----------------------------------------------
Fastswitch packets from: Fast-Ethernet to Fast-Ethernet
- Min Time: 0 micro seconds
  - Avg Time: 0 micro seconds
  - Max Time: 0 micro seconds
- Total number Fastswitch-packets: 0
- Number of packets from output queue (non-Fastswitch): 0

<table>
<thead>
<tr>
<th>Perf Ctr Min</th>
<th>Perf Ctr Avg</th>
<th>Perf Ctr Max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clock Cycles</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total-Issued Instructions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Floating Point Instructions Issued</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Integer Instructions Issued</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Load Instructions Issued</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Store Instructions Issued</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dual-Issued Instruction Pairs</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Branch Pre-Fetches</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Slip Cycles</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Stall Cycles</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>On-Chip Secondary Cache Misses</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Primary Instruction Cache Misses</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Primary Data Cache Misses</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show platform

To display platform information, use the **show platform** command in privileged EXEC mode.

```
show platform {buffers|copp rate-limit
              |arp|dhcp|atm-oam|ethernet-oam|icmp|igmp|pppoe-discovery|atom ether-vc|all}|np copp [ifnum]
              |detail|dma|eeprom|fault|hardware capacity|hardware pfc
mode|internal-vlan| interrupts| netint|software ipv6-multicast connected| stats| tech-support {ipmulticast
             [vrf vrf-name] group-ip-addr src-ip-addr|unicast [vrf vrf-name] destination-ip-addr destination-mask
             [global]|tlb|vfi \|tlb|vfi dot1q-transparency|vlans}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffers</td>
<td>Displays buffer-allocation information.</td>
</tr>
<tr>
<td>copp rate-limit</td>
<td>Displays Cisco Control Plane Policing (CoPP) rate-limit information on the</td>
</tr>
<tr>
<td></td>
<td>Cisco 7600 SIP-400.</td>
</tr>
<tr>
<td>arp</td>
<td>Specifies Address Resolution Protocol (ARP) packet traffic.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Specifies Dynamic Host Configuration Protocol (DHCP) packet traffic.</td>
</tr>
<tr>
<td>atm-oam</td>
<td>Specifies ATM Operation, Administration, and Maintenance (OAM) packet</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td>ethernet-oam</td>
<td>Specifies Ethernet OAM packet traffic.</td>
</tr>
<tr>
<td>icmp</td>
<td>Specifies Internet Connection Management Protocol Rate limiter.</td>
</tr>
<tr>
<td>igmp</td>
<td>Specifies Internet Group Management Protocol Rate limiter.</td>
</tr>
<tr>
<td>pppoe-discovery</td>
<td>Specifies Point-to-Point Protocol over Ethernet (PPPoE) discovery packet</td>
</tr>
<tr>
<td></td>
<td>information.</td>
</tr>
<tr>
<td>atom ether-vc</td>
<td>Shows whether IP or routed mode interworking is configured.</td>
</tr>
<tr>
<td>all</td>
<td>Displays rate-limit information for all protocols.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>np copp</td>
<td>Displays debug information for a given CoPP session ID or for all CoPP sessions.</td>
</tr>
<tr>
<td>ifnum</td>
<td>(Optional) A session ID.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Shows full rate-limited values.</td>
</tr>
<tr>
<td>dma</td>
<td>Displays Direct Memory Access (DMA) channel information.</td>
</tr>
<tr>
<td>eeprom</td>
<td>Displays CPU EEPROM information.</td>
</tr>
<tr>
<td>fault</td>
<td>Displays the fault date.</td>
</tr>
<tr>
<td>hardware capacity</td>
<td>Displays the capacities and utilizations for hardware resources; see the show platform hardware capacity command.</td>
</tr>
<tr>
<td>hardware pfc mode</td>
<td>Displays the type of installed Policy Feature Card (PFC).</td>
</tr>
<tr>
<td>internal-vlan</td>
<td>Displays the internal VLAN.</td>
</tr>
<tr>
<td>interrupts</td>
<td>Displays m8500 interrupt counters.</td>
</tr>
<tr>
<td>netint</td>
<td>Displays the platform network-interrupt information.</td>
</tr>
<tr>
<td>software ipv6-multicast connected</td>
<td>Displays all the IPv6 subnet Access Control List (ACL) entries on the Route Processor (RP); see the show platform software ipv6-multicast command.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays Constellation WAN (CWAN) statistics.</td>
</tr>
<tr>
<td>tech-support ipmulticast</td>
<td>Displays IP multicast-related information for Technical Assistance Center (TAC).</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Displays the Virtual Private Network (VPN) routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>group-ip-addr</td>
<td>Group IP address.</td>
</tr>
<tr>
<td>src-ip-addr</td>
<td>Source IP address.</td>
</tr>
<tr>
<td>unicast</td>
<td>Displays IP unicast-related information for TAC.</td>
</tr>
<tr>
<td>destination-ip-addr</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td>destination-mask</td>
<td>Destination mask.</td>
</tr>
<tr>
<td>global</td>
<td>(Optional) Displays global output.</td>
</tr>
<tr>
<td>tlb</td>
<td>Displays information about the translation look-aside buffer (TLB) register.</td>
</tr>
<tr>
<td>vfi</td>
<td>Displays CWAN virtual forwarding instance (VFI) commands.</td>
</tr>
<tr>
<td>dot1q-transparency</td>
<td>Displays the dot1q transparency setting.</td>
</tr>
<tr>
<td>vlans</td>
<td>Displays hidden VLAN-to-WAN interface mapping.</td>
</tr>
</tbody>
</table>
Privileged EXEC (#)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Cisco</td>
</tr>
<tr>
<td></td>
<td>IOS Release 12.2(17d)SXB. This command was changed to include the</td>
</tr>
<tr>
<td></td>
<td>hardware pfc mode keywords.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was modified to include the software ipv6-multicast</td>
</tr>
<tr>
<td></td>
<td>connected keywords.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was modified to include additional keywords to support CoPP</td>
</tr>
<tr>
<td></td>
<td>enhancements on the Cisco 7600 SIP-400 on the Cisco 7600 series router.</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>XE Release 2.1</td>
<td></td>
</tr>
<tr>
<td>12.2(33)SRD</td>
<td>This command was modified. The atom ether-vc keyword was added.</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
<tr>
<td>XE Release 3.9S</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is similar to the **show msfc** command.

This command can be used to verify the existence of a second Cisco IOS process on a single Cisco ASR 1000 RP on a Cisco ASR 1002 router or Cisco ASR 1004 router.

When this command is used with the atom ether-vc keyword, it is used on the line-card console.

**Examples**

The following sample output from the **show platform buffers** command displays buffer-allocation information:

```
Router# show platform buffers
Reg. set  Min  Max
TX         640
ABQ  640  16384
  0   0  40
  1  6715  8192
  2   0   0
  3   0   0
  4   0   0
  5   0   0
  6   0   0
  7   0   0
Threshold  = 8192
Vlan Sel Min  Max  Cnt  Rsvd
 1019  1  6715  8192  0  0
Router#
```
Cisco ISR 4400 Series Routers

The following example displays online status information for the Cisco ISR 4400 Front Panel Gigabit Ethernet port (ISR4451-4X1GE), Cisco SSD Carrier Card Network Interface Module (NIM-SSD), Cisco SM-1T3/E3 Service Module (SM-1T3/E3), and Cisco 4th Generation T1/E1 Voice and WAN Network Interface Module (NIM 8MFT-T1/E1).

Router# show platform
Chassis type: ISR4452/K9

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Insert time (ago)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ISR4452/K9</td>
<td>ok</td>
<td>15:57:33</td>
</tr>
<tr>
<td>0/0</td>
<td>ISR4451-4X1GE</td>
<td>ok</td>
<td>15:55:24</td>
</tr>
<tr>
<td>0/3</td>
<td>NIM-SSD</td>
<td>ok</td>
<td>15:55:24</td>
</tr>
<tr>
<td>1</td>
<td>ISR4452/K9</td>
<td>ok</td>
<td>15:57:33</td>
</tr>
<tr>
<td>1/0</td>
<td>NIM 8MFT-T1/E1</td>
<td>ok</td>
<td>15:55:24</td>
</tr>
<tr>
<td>2</td>
<td>ISR4452/K9</td>
<td>ok</td>
<td>15:57:33</td>
</tr>
<tr>
<td>2/0</td>
<td>SM-1T3/E3</td>
<td>ok</td>
<td>15:55:24</td>
</tr>
<tr>
<td>R0</td>
<td>ISR4452/K9</td>
<td>ok, active</td>
<td>15:57:33</td>
</tr>
<tr>
<td>F0</td>
<td>ISR4451-FP</td>
<td>ok, active</td>
<td>15:57:33</td>
</tr>
<tr>
<td>F0</td>
<td>Unknown</td>
<td>ps, fail</td>
<td>never</td>
</tr>
<tr>
<td>P1</td>
<td>XXX-XXXX-XX</td>
<td>ok</td>
<td>15:56:58</td>
</tr>
<tr>
<td>P2</td>
<td>ACS-4450-ASSY</td>
<td>ok</td>
<td>15:56:58</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot</th>
<th>CPLD Version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>12090323</td>
<td>15.3(01r)S</td>
</tr>
<tr>
<td>1</td>
<td>12090323</td>
<td>15.3(01r)S</td>
</tr>
<tr>
<td>2</td>
<td>12090323</td>
<td>15.3(01r)S</td>
</tr>
<tr>
<td>R0</td>
<td>12090323</td>
<td>15.3(01r)S</td>
</tr>
<tr>
<td>F0</td>
<td>12090323</td>
<td>15.3(01r)S</td>
</tr>
</tbody>
</table>

The table below describes the fields that appear in the above example

**Table 134: Show Platform Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>slot number</td>
</tr>
<tr>
<td>Type</td>
<td>Type of module</td>
</tr>
<tr>
<td>State</td>
<td>Status of the module</td>
</tr>
<tr>
<td>Insert Time</td>
<td>Period of time ((hh:mm:ss format) since the module has been up and running</td>
</tr>
</tbody>
</table>

Cisco ASR 1000 Series Routers

The following example displays online status information for the shared port adapters (SPAs), Cisco ASR 1000 SPA Interface Processor (SIP), Cisco ASR 1000 Embedded Services Processor (ESP), Cisco ASR 1000 RP, power supplies, and fans. The ESPs are shown as F0 and F1. The RPs are shown as R0 and R1.

The State column should display “ok” for SIPs, SPAs, power supplies, and fans. For RPs and ESPs, the State column should display “ok, active” or “ok, standby.”
Cisco ASR 1000 Series Routers--Verifying Dual Cisco IOS Processes on Single RP

In the following example, a second Cisco IOS process is enabled on a Cisco ASR 1004 router using stateful switchover (SSO). The output of the `show platform` command is provided before and after the SSO configuration to verify that the second Cisco IOS process is enabled and active.

```
Router# show platform
Chassis type: ASR1004
Slot | Type | State | Insert time (ago)
-----|------|-------|-------------------
0    | ASR1000-SIP10 | ok     | 00:04:39
0/0  | SPA-5X1GE-V2   | ok     | 00:03:23
0/1  | SPA-8X1FE-TX-V2| ok     | 00:03:18
0/2  | SPA-2XCT3/DSO  | ok     | 00:03:39
1    | ASR1000-SIP10  | ok, active | 00:04:39
1/0  | SPA-2XOC3-POS  | ok, standby | 00:03:18
1/1  | SPA-8XCHT1/E1 | ok     | 00:03:18
1/2  | SPA-2XT3/E3   | ok     | 00:03:18
R0   | ASR1000-RP1    | ok, active | 00:04:39
R1   | ASR1000-RP1    | ok, standby | 00:03:18
F0   | ASR1000-ESP10  | ok, active | 00:03:52
F1   | ASR1000-ESP10  | ok, standby | 00:03:52
P0   | ASR1004-PWR-AC | ok     | 00:03:52
P1   | ASR1004-PWR-AC | ok     | 00:03:52
Slot | CPLD Version   | Firmware Version
-----|----------------|-------------------
0    | 07091401       | 12.2 (33r) XN2
R0   | 07062111       | 12.2 (33r) XN2
F0   | 07051680       | 12.2 (33r) XN2
```

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# redundancy

*May 27 19:43:43.539: %CMRP-6-DUAL_IOS_REBOOT_REQUIRED: R0/0: cmd: Configuration must be saved and the chassis must be rebooted for IOS redundancy changes to take effect
```

```
Router(config-red)# exit
Router(config)# exit
Router# copy running-config startup-config
```

show platform

Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
<reload output omitted for brevity>
Router# show platform
Chassis type: ASR1004
Slot Type State Insert time (ago)------------------ ----------------- --------------------- ------------------
0 ASR1000-SIP10 ok 00:29:34
0/0 SPA-5X1GE-V2 ok 00:28:13
0/1 SPA-2XT3/E3 ok 00:28:18
R0 ASR1000-RP1 ok 00:29:34 R0/0 ok, active 00:29:34
00:27:49 F0 ASR1000-ESP10 ok, active 00:29:34
P0 ASR1004-PWR-AC ok 00:28:47
P1 ASR1004-PWR-AC ok 00:28:47
Slot CPLD Version Firmware Version
--------- ------------------- ---------------------------------------
0 07091401 12.2(33r)XN2
R0 07062111 12.2(33r)XN2
F0 07051680 12.2(33r)XN2

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>Chassis slot.</td>
</tr>
<tr>
<td>Type</td>
<td>Hardware type.</td>
</tr>
</tbody>
</table>

Cisco IOS Configuration Fundamentals Command Reference
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Online state of the hardware. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>All Hardware</td>
</tr>
<tr>
<td></td>
<td>• booting--Hardware is initializing and software is booting.</td>
</tr>
<tr>
<td></td>
<td>• disabled--Hardware is not operational.</td>
</tr>
<tr>
<td></td>
<td>• init--Hardware or Cisco IOS process is initializing.</td>
</tr>
<tr>
<td></td>
<td>• ok--Hardware is operational.</td>
</tr>
<tr>
<td></td>
<td>• shutdown--Hardware was administratively shut down using the no shutdown</td>
</tr>
<tr>
<td></td>
<td>command.</td>
</tr>
<tr>
<td></td>
<td>• unknown--Hardware is not operational; state is unknown.</td>
</tr>
<tr>
<td>RP or ESP</td>
<td>init, standby--Standby RP or ESP is operational but is not yet in a high availability (HA) state. An RP or ESP switchover is not yet possible.</td>
</tr>
<tr>
<td></td>
<td>ok, active--Active RP or ESP is operational.</td>
</tr>
<tr>
<td></td>
<td>ok, standby--Standby RP or ESP is operational. The standby RP or ESP is ready to become active in the event of a switchover.</td>
</tr>
<tr>
<td>SPA</td>
<td>admin down--SPA was disabled using the shutdown command.</td>
</tr>
<tr>
<td></td>
<td>inserted--SPA is being inserted.</td>
</tr>
<tr>
<td></td>
<td>missing--SPA was removed.</td>
</tr>
<tr>
<td></td>
<td>out of service--SPA is not operational.</td>
</tr>
<tr>
<td></td>
<td>retrieval error--An error occurred while retrieving the SPA state; state is unknown.</td>
</tr>
<tr>
<td></td>
<td>stopped--SPA was gracefully deactivated using the hw-module subslot stop command.</td>
</tr>
<tr>
<td>Fan or Power Supply</td>
<td>fan, fail--Fan is failing.</td>
</tr>
<tr>
<td></td>
<td>ps, fail--Power supply is failing.</td>
</tr>
<tr>
<td>Insert time (ago)</td>
<td>Amount of time (hh:mm:ss format) the hardware has been online.</td>
</tr>
<tr>
<td>CPLD Version</td>
<td>Complex programmable logic device version number.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Firmware (ROMmon) version number.</td>
</tr>
</tbody>
</table>
Cisco 7600 Series Routers with Cisco 7600 SIP-400

The following sample output from the `show platform copp rate-limit arp` command displays the list of interfaces on which a rate limiter is active for ARP, along with the count of confirmed and exceeded packets for the rate limiter:

```
Router# show platform copp rate-limit arp
Rate limiter Information for Protocol arp:
  Rate Limiter Status: Enabled
  Rate : 20 pps
  Max Observation Period : 60 seconds
Per Interface Rate Limiter Information
  Interface               Conformed Pkts Exceeded Pkts Enabled Obs Period (Mts)
  GigabitEthernet5/1        0       0       No       -
  GigabitEthernet5/1.1      14       0       No       -
  GigabitEthernet5/1.2      28       2       No       -
  GigabitEthernet5/2         0       0       No       -
  GigabitEthernet5/2.1     180       4       Yes      35
  GigabitEthernet5/2.2     200      16       Yes      Max
```

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

### Table 136: show platform copp rate-limit Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limiter Status</td>
<td>Indicates if a rate limiter has been enabled on the interface.</td>
</tr>
<tr>
<td>Rate</td>
<td>Indicates the configured rate in packets per second (pps) or bits per second (bps).</td>
</tr>
<tr>
<td>Max Observation Period</td>
<td>Indicates the configured observation period, in seconds, before the per-interface rate limiter is automatically turned off.</td>
</tr>
<tr>
<td>Per Interface Rate Limiter Information</td>
<td>Displays the list of interfaces on which the rate limiter is active. In this example:</td>
</tr>
<tr>
<td></td>
<td>• GigabitEthernet5/1.1 is free from attack.</td>
</tr>
<tr>
<td></td>
<td>• GigabitEthernet5/2.1 has an exceed count of 4, and has a rate limiter enabled. The observation period is 35 minutes, which indicates that currently the interface is free from attack and is being kept under observation. The interface will remain under observation for an additional 35 minutes. If it remains free from attack after that time, the rate limiter is automatically removed.</td>
</tr>
<tr>
<td></td>
<td>• GigabitEthernet5/2.2 has an exceed count of 16 and has a rate limiter enabled. The observation period has been designated as Max. This indicates that the interface is still under attack and has not yet entered the observation time window.</td>
</tr>
</tbody>
</table>

The following sample from the `show platform eeprom` command displays CPU EEPROM information:

```
Router# show platform eeprom
MSFC CPU IDPROM:
  IDPROM image:
  IDPROM image block #0:
```
show monitor permit list through show process memory
show platform

hexadecimal contents of block:
00: AB AB 02 9C 13 5B 02 00 00 02 60 03 03 E9 43 69
.....[....`...Ci
10: 73 63 6F 20 53 79 73 74 65 6D 73 00 00 00 00 00
sco Systems.....
20: 00 00 57 53 2D 58 36 4B 2D 53 55 50 33 2D 50 46
..WS-X6K-SUP3-PF
30: 43 33 00 00 00 00 53 41 44 30 36 34 34 30 31 57
C3....SAD064401W
40: 4C 00 00 00 00 00 00 00 00 00 37 33 2D 37 34 30
L.........73-740
50: 34 2D 30 37 00 00 00 00 00 00 30 35 00 00 00 00
4-07......05....
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
70: 00 00 00 00 02 BD 00 00 00 00 00 09 00 05 00 01
................
80: 00 03 00 01 00 01 00 02 03 E9 00 00 00 00 00 00
................
90: 00 00 00 00 00 00 00 00 00 00 00 00
............
block-signature = 0xABAB, block-version = 2,
block-length = 156, block-checksum = 4955
*** common-block ***
IDPROM capacity (bytes) = 512 IDPROM block-count = 2
FRU type = (0x6003,1001)
OEM String = 'Cisco Systems'
Product Number = 'WS-X6K-SUP3-PFC3'
Serial Number = 'SAD064401WL'
Manufacturing Assembly Number = '73-7404-07'
Manufacturing Assembly Revision = '05'
Hardware Revision = 0.701
Manufacturing bits = 0x0 Engineering bits = 0x0
SNMP OID = 9.5.1.3.1.1.2.1001
Power Consumption = 0 centiamperes
RMA failure code = 0-0-0-0
CLEI =
*** end of common block ***
IDPROM image block #1:
hexadecimal contents of block:
00: 60 03 02 67 0C 24 00 00 00 00 00 00 00 00 00 00
`..g.$..........
10: 00 00 00 00 00 00 00 51 00 05 9A 3A 7E 9C 00 00
.......Q...:~...
20: 02 02 00 01 00 01 00 00 00 00 00 00 00 00 00 00
................
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
40: 14 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
50: 00 00 81 81 81 81 80 80 80 80 80 80 80 80 80 80
................
60: 80 80 06 72 00 46 37
...r.F7
block-signature = 0x6003, block-version = 2,
block-length = 103, block-checksum = 3108
*** linecard specific block ***
feature-bits =
00000000 00000000
hardware-changes-bits =
00000000 00000000
card index = 81
mac base = 0005.9A3A.7E9C
mac_len = 0
num_processors = 2
epld_num = 2
epld_versions = 0001 0001 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
port numbers:
pair #0: type=14, count=01
pair #1: type=00, count=00
pair #2: type=00, count=00
pair #3: type=00, count=00
pair #4: type=00, count=00
pair #5: type=00, count=00
pair #6: type=00, count=00
pair #7: type=00, count=00
sram_size = 0
sensor_thresholds =
sensor #0: critical = -127 oC (sensor present but ignored), warning = -127 oC (sensor
present but ignored)
sensor #1: critical = -127 oC (sensor present but ignored), warning = -127 oC (sensor
present but ignored)
sensor #2: critical = -128 oC (sensor not present), warning = -128 oC (sensor not

Cisco IOS Configuration Fundamentals Command Reference
789


sensor #3: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #4: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #5: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #6: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
sensor #7: critical = -128 oC (sensor not present), warning = -128 oC (sensor not present)
max_connector_power = 1650
cooling_requirement = 70
ambient_temp = 55

The following sample output from the `show platform fault` command displays fault-date information:

Router# show platform fault
Fault History Buffer:
   rsp72043_rp Software (rsp72043_rp-ADVENTERPRISEK9_DBG-M), Version 12.2(32.8.1)RE
   Cl86 ENGINEERING WEEKLY BUILD, synced to V122_32_8_11_SR186
   Compiled Wed 08-Apr-09 09:22 by abcd
   Uptime 2w3d
   Exception Vector: 0x1500 PC 0x0B13DD4C MSR 0x00029200 LR 0x0B13DD10
   r0 0x0B13DD10 r1 0x1C58A1C8 r2 0xFFFFFCFFFC r3 0x189EDEF4
   r4 0x00000000 r5 0x00000000 r6 0x1C58A1B0 r7 0x00029200
   r8 0x00029200 r9 0x00000000 r10 0x00000001 r11 0x189EDEF0
   r12 0x00000000 r13 0x00044000 r14 0x08736008 r15 0x115C0000
   r16 0x00000000 r17 0x00000000 r18 0x00000000 r19 0x18751358
   r20 0x00000000 r21 0x00000000 r22 0x00000000 r23 0x00000000
   r24 0x00000000 r25 0x00000000 r26 0x00000000 r27 0x00000001
   r28 0x13255EC0 r29 0x1C59BD00 r30 0x13255EC0 r31 0x00000000
dec 0x00000733 tbu 0x00000460 tbl 0x594BBFC4 pvr 0x80210020
dear 0x00000000 dbcr0 0x41100000 dbcr1 0x00000000 dbcr2 0x00000000
   lac1 0x00000000 lac2 0x00000000 dac1 0x00000000 dac2 0x00000000

The following sample output from the `show platform hardware pfc` mode command displays the PFC-operating mode:

Router# show platform hardware pfc mode
PFC operating mode : PFC3A

This example shows how to display platform network-interrupt information:

Router# show platform netint
Network IO Interrupt Throttling:
  throttle count=0, timer count=0
  active=0, configured=1
  netint usec=3999, netint mask usec=800
  inband_throttle_mask_hi = 0x0
  inband_throttle_mask_lo = 0x800000

This following sample output from the `show platform tlb` command displays the TLB-register information:

Router# show platform tlb
Mistral revision 5
TLB entries : 42

<table>
<thead>
<tr>
<th>Virt Address range</th>
<th>Phy Address range</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x10000000:0x1001FFFF</td>
<td>0x010000000:0x01001FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x10020000:0x1003FFFF</td>
<td>0x010020000:0x01003FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x10040000:0x1005FFFF</td>
<td>0x010040000:0x01005FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x10060000:0x1007FFFF</td>
<td>0x010060000:0x01007FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x10080000:0x10087FFF</td>
<td>0x010080000:0x010087FFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x10088000:0x1008FFFF</td>
<td>0x010088000:0x01008FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x18000000:0x1801FFFF</td>
<td>0x010000000:0x01001FFFF</td>
<td>CacheMode=0, RW, Valid</td>
</tr>
<tr>
<td>0x19000000:0x1901FFFF</td>
<td>0x010000000:0x01001FFFF</td>
<td>CacheMode=7, RW, Valid</td>
</tr>
<tr>
<td>0x1E000000:0x1E1FFFFF</td>
<td>0x01E000000:0x01E1FFFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x1E880000:0x1E899FFF</td>
<td>0x01E880000:0x01E8999FF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x1FC00000:0x1FC7FFFF</td>
<td>0x01FC00000:0x01FC7FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x30000000:0x3001FFFF</td>
<td>0x070000000:0x07001FFFF</td>
<td>CacheMode=2, RW, Valid</td>
</tr>
<tr>
<td>0x40000000:0x407FFFFF</td>
<td>0x000000000:0x0007FFFFF</td>
<td>CacheMode=3, RO, Valid</td>
</tr>
<tr>
<td>0x58000000:0x59FFFFFF</td>
<td>0x088000000:0x089FFFFFF</td>
<td>CacheMode=3, RW, Valid</td>
</tr>
<tr>
<td>0x5A000000:0x5BFFFFFF</td>
<td>0x08A000000:0x08BFFFFF</td>
<td>CacheMode=3, RW, Valid</td>
</tr>
<tr>
<td>0x5C000000:0x5DFFFFFF</td>
<td>0x08C000000:0x08DFFFFF</td>
<td>CacheMode=3, RW, Valid</td>
</tr>
<tr>
<td>0x5E000000:0x5FFFFFFF</td>
<td>0x08E000000:0x08FFFFFF</td>
<td>CacheMode=3, RW, Valid</td>
</tr>
</tbody>
</table>

This example shows how use the `atom ether-vc` keyword to display line-card information for an ES20 line card in slot 3.

Router# show platform copp rate-limit atom ether-vc

**AToM Ether VC Index (12902):** segtype(3) seghandle(0x5ECF7F34)

**Disposition:** flags(97) vlanid(502) local_vc_label(22691)

**ForwardingTable:** oper(12) flags(0x2100) vlan(502) dest_index(0x9ED)

**Imposition:** flags(0x21) egress_idx(0x0) ifnum(28)

**tx_tvc:** (0x7083) rvcbl[0](3356) rigplbl[1](1011) label[2](0)

**label[3](0) ltl[0x9ED] mac(014.1c80.f600) qos_info(0x0)

**Platform Data:**

```
loc_lbl acif_num fw_idx cword eg_ifnum ckt_idx vlan ac_hdl vl vc_hash
22691 615 0x0 0x3 28 0x8003 502 0x5ECF7F34 0x3266
```

**Platform Index:** (0x81F68003) is_sw(1) is_vfi(0) vlan(502) pseudo_port_offset(3) tx_tvc(0x7D83)

**Statistics:**

```
Packets Bytes Drop Pkt Drop Bytes ID
Disposition: 0 0 0 0 0
Imposition: 0 0 0 0 0
```

**Vlan func[1]:** 502 (0x1F6) func(0:invalid) feat (0x0)

```
T x TVC Table
idx ltl h pt cw vt efp adj v imp
x-- x-- d-- d-- d-- d-- x-- x--
```

**SIP10G EoMPLS disp detailed info:**

```
t vcbl VLAN Type disp-idx
  - d------ x--(d---) ------ x------
0 00022691 01F6(0502) ether 00001692
```

**SIP10G EoMPLS ipiw disp detailed info:**

```
piw mac valid CE-MAC Address
  b--- b-------- --------------
0001 0000000001 0016.9c6e.7480
```

**VC Summary:** vlan(502) VC count(1)

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>platform copp</strong></td>
<td>Turns on or off rate-limiting for an interface on the Cisco 7600 SIP-400.</td>
</tr>
</tbody>
</table>
show platform bridge

To display distributed or hardware-based bridging information, use the `show platform bridge` command in privileged EXEC mode.

```
show platform bridge [interface-type interface-number] [vlan vlan-id] [summary]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type and number.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Displays VLAN bridging information.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(Optional) Displays a summary of bridging information.</td>
</tr>
</tbody>
</table>

**Command Modes**  
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show platform bridge` command:

```
Router# show platform bridge
VLAN Interface CircuitId LTL PseudoPort State Options
12 PO1/1/3.1 102 0xC3F 1/256 up dot1q
13 PO1/1/3.1 103 0xC3F 1/256 up dot1q
14 PO1/1/3.2 104 0xC3F 1/256 up default
15 PO1/1/3.2 105 0xC3F 1/256 up default
16 PO1/1/3.3 106 0xC3F 1/256 up dot1q-tunnel
17 PO1/1/3.3 107 0xC3F 1/256 up dot1q-tunnel
41 G18/0/17 1201 0xDE2 8/227 up access
41 G18/0/17 1202 0xDE3 8/228 up access
41 G18/0/17 1203 0xDE4 8/229 up access
41 G18/0/17 1204 0xDE5 8/230 up access
41 G18/0/17 1205 0xDE6 8/231 up access
41 G18/0/17 1206 0xDE7 8/232 up access
41 G18/0/17 1207 0xDE8 8/233 up access
41 G18/0/17 1208 0xDE9 8/234 up access
41 G18/0/17 1209 0xDEA 8/235 up access
41 G18/0/17 1210 0 STDOUT 8/236 up access
41 G18/0/17 1211 0xDEC 8/237 up access
41 G18/0/17 1212 0xDED 8/238 up access
41 G18/0/17 1213 0 STDERR 8/239 up access
41 G18/0/17 1214 0xDEE 8/240 up access
41 G18/0/17 1215 0xDF0 8/241 up access
```
The table below describes the significant fields shown in the display.

### Table 137: show platform bridge Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>The VLAN for which bridging is configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>The WAN interface on which bridging is configured. This can be an ATM, Gigabit Ethernet, POS, or Serial interface.</td>
</tr>
<tr>
<td>CircuitId</td>
<td>The circuit ID. The range is from 0 to 65536.</td>
</tr>
<tr>
<td>LTL</td>
<td>The local target logic (LTL) of the interface. LTL is 13 bits long. The format is eee ssss pppppp (e: extended port bits, s: slot bits, p: port bits). Extended bits along with port bits identify the pseudoport and slot bits identifies the slot.</td>
</tr>
<tr>
<td>PseudoPort</td>
<td>In the case of flexwan, the port numbering is from 133 to 192 for Bay 0 and 197 to 256 for Bay 1. There are 60 ports per packet processing engine (PPE). For the SIP200, the pseudoports are in the range of 137 to 256.</td>
</tr>
<tr>
<td>State</td>
<td>State indicates the status of the physical interface on which bridging is configured. The state is either up or down. If the state is down, then there is a problem and debugging needs to be done.</td>
</tr>
<tr>
<td>Options</td>
<td>Options specify whether split-horizon is enabled on the WAN interface. This can be access, default, dot1q, or dot1q-tunnel.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
</tbody>
</table>

### show platform cfm

To display connectivity fault management (CFM) commands, use the `show platform cfm` command in privileged EXEC mode.

```
show platform cfm {epl|info|interface {fastethernet|gigabitethernet|port-channel} number {fwd_vlan vlan-number|level|vlan_list}}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>epl</td>
<td>Displays CFM Ethernet private line (EPL) details.</td>
</tr>
<tr>
<td>info</td>
<td>Displays the CFM Platform Adaptation Layer (PAL) information.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies the interface type.</td>
</tr>
<tr>
<td>fastethernet</td>
<td>Specifies the FastEthernet interface.</td>
</tr>
<tr>
<td>gigabitethernet</td>
<td>Specifies the GigabitEthernet interface.</td>
</tr>
<tr>
<td>port-channel</td>
<td>Specifies the port-channel interface.</td>
</tr>
</tbody>
</table>
number Interface number.

fwd_vlan Displays the CFM forward VLAN list.

vlan-number VLAN number.

level Displays the CFM level for the interface.

vlan_list Specifies CFM VLAN list.

Command Modes
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the `show platform cfm info` command. The field descriptions are self-explanatory.

```
Router# show platform cfm info
CFM is disabled
CFM unicast MAC 00d0.2b6c.b103, CFM multicast MAC 0180.c200.0030, AEB multicast MAC 0100.0ccc.ccc0
CFM Ingress Control Packet System Statistics:
  Current software Rate Limit Setting: 1100 pkts/sec
  Statistics are collected in intervals of 3 seconds.
  Allow the first 3300 packets to pass each interval, drop thereafter
  Current Ingress Count in this interval: 0 pkts
  In this interval have we Exceeded Rate and Dropped pkts: NO
  For the last 3 intervals the maximum sample had 0 packets in one interval.
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
</tbody>
</table>

show platform diag

To display diagnostic and debug information for individual platform components, use the `show platform diag` command in privileged EXEC mode.

```
show platform diag
```

Syntax Description

diag Displays diagnostic and debug information for the platform components.

Command Default

This command has no default settings.

Command Modes

privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.2</td>
<td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command can be used to display debug and diagnostic information and indicate the status of field replaceable unit (FRU) components in any Cisco ASR 1000 Series Router.

Examples

The following example displays diagnostic information for the Cisco ASR 1000 SPA Interface Processor (SIP), shared port adapters (SPAs), Cisco ASR 1000 Embedded Services Processor (ESP), Cisco ASR 1000 Route Processors (RP), and power supplies. The ESP is shown as F0 or F1. The RPs are shown as R0 or R1. The power supplies are shown as P0 and P1.

```
Router# show platform diag

Chassis type: ASR1004
Slot: 0, ASR1000-SIP10
  Running state : ok
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:00:48 (4d22h ago)
  Software declared up time : 00:01:40 (4d22h ago)
  CPLD version : 07091401
  Firmware version : 12.2(33r)XNB
  Sub-slot: 0/0, SPA-5X1GE-V2
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:00:36 (4d22h ago)
    Logical insert detect time : 00:02:23 (4d22h ago)
  Slot: R0, ASR1000-RP1
    Running state : ok
    Internal state : online
    Internal operational state : ok
    Physical insert detect time : 00:00:48 (4d22h ago)
    Software declared up time : 00:00:48 (4d22h ago)
    CPLD version : 07062111
    Firmware version : 12.2(33r)XNB
    Sub-slot: R0/0,
      Running state : ok, active
      Logical insert detect time : 00:00:48 (4d22h ago)
      Became HA Active time : 00:04:56 (4d22h ago)
    Sub-slot: R0/1,
      Running state : ok, standby
    Logical insert detect time : 00:02:50 (4d22h ago)
  Slot: F0, ASR1000-ESP10
    Running state : ok, active
    Internal state : online
    Internal operational state : ok
    Physical insert detect time : 00:00:48 (4d22h ago)
    Software declared up time : 00:01:40 (4d22h ago)
    Hardware ready signal time : 00:00:49 (4d22h ago)
    Packet ready signal time : 00:01:49 (4d22h ago)
    CPLD version : 07051680
    Firmware version : 12.2(33r)XNB
```
Slot: P0, ASR1004-PWR-AC
State: ok
Physical insert detect time: 00:01:40 (4d22h ago)
Slot: P1, ASR1004-PWR-AC
State: ok
Physical insert detect time: 00:01:40 (4d22h ago)

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

### Table 138: show platform diag Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running state</td>
<td>The current online running state of the FRU component.</td>
</tr>
<tr>
<td>Internal state</td>
<td>The internal debug state of the FRU component for diagnostic purposes.</td>
</tr>
<tr>
<td>Internal operational state</td>
<td>The internal operational state of the FRU component for diagnostic purposes.</td>
</tr>
<tr>
<td>Physical insert detect time</td>
<td>The time of the most recent physical insertion of the FRU component detected by the platform code.</td>
</tr>
<tr>
<td>Software declared up time</td>
<td>The time that the software on the FRU component was declared running by the platform code.</td>
</tr>
<tr>
<td>Hardware ready signal time</td>
<td>The time that the hardware ready signal was detected by the platform code.</td>
</tr>
<tr>
<td>Packet ready signal time</td>
<td>The time that the Embedded Service Processor (ESP) packet ready signal was detected by the platform code.</td>
</tr>
<tr>
<td>CPLD version</td>
<td>The Complex Programmable Logic Device version number.</td>
</tr>
<tr>
<td>Firmware version</td>
<td>The Firmware (ROMmon) version number.</td>
</tr>
<tr>
<td>Logical insert detect time</td>
<td>The time that the SPA was logically detected by the platform code.</td>
</tr>
<tr>
<td>Became HA Active time</td>
<td>The time that this FRU became High Availability (HA) active status.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
<tr>
<td>show platform hardware</td>
<td>Displays platform hardware information.</td>
</tr>
<tr>
<td>show platform software</td>
<td>Displays platform software information</td>
</tr>
</tbody>
</table>

### show platform hardware capacity

To display the capacities and utilizations for the hardware resources, use the `show platform hardware capacity` command in privileged EXEC mode.

```
show platform hardware capacity [resource-type]
```
Syntax Description

| resource-type | (Optional) Hardware resource type; see the “Usage Guidelines” section for the valid values. |

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXF</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI. Support was added for the ibc and rewrite-engine keywords.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The valid values for resource-type are as follows:

- acl --Displays the capacities and utilizations for ACL/QoS TCAM resources.
- cpu --Displays the capacities and utilizations for CPU resources.
- eobc --Displays the capacities and utilizations for Ethernet out-of-band channel resources.
- fabric --Displays the capacities and utilizations for Switch Fabric resources.
- flash --Displays the capacities and utilizations for Flash/NVRAM resources.
- forwarding --Displays the capacities and utilizations for Layer 2 and Layer 3 forwarding resources.
- ibc --Displays the capacities and utilizations for interboard communication resources.
- interface --Displays the capacities and utilizations for interface resources.
- monitor --Displays the capacities and utilizations for SPAN resources.
- multicast --Displays the capacities and utilizations for Layer 3 multicast resources.
- netflow --Displays the capacities and utilizations for NetFlow resources.
- pfc --Displays the capacities and utilizations for all the PFC resources including Layer 2 and Layer 3 forwarding, NetFlow, CPU rate limiters, and ACL/QoS TCAM resources.
- power --Displays the capacities and utilizations for power resources.
- qos --Displays the capacities and utilizations for QoS policer resources.
- rate-limit --Displays the capacities and utilizations for CPU rate limiter resources.
- rewrite-engine --Displays the packet drop and performance counters of the central rewrite engine on supervisors and line cards. For detailed information, see the show platform hardware capacity rewrite-engine command documentation.
- system --Displays the capacities and utilizations for system resources.
- vlan --Displays the capacities and utilizations for VLAN resources.

The show platform hardware capacity cpu command displays the following information:
• CPU utilization for the last 5 seconds (busy time and interrupt time), the percentage of the last 1-minute average busy time, and the percentage of the last 5-minute average busy time.
• Processor memory total available bytes, used bytes, and percentage used.
• I/O memory total available bytes, used bytes, and percentage used.

The `show platform hardware capacity` command displays the following information:
• Transmit and receive rate
• Packets received and packets sent
• Dropped received packets and dropped transmitted packets

The `show platform hardware capacity forwarding` command displays the following information:
• The total available entries, used entries, and used percentage for the MAC tables.
• The total available entries, used entries, and used percentage for the FIB TCAM tables. The display is done per protocol base.
• The total available entries, used entries, and used percentage for the adjacency tables. The display is done for each region in which the adjacency table is divided.
• The created entries, failures, and resource usage percentage for the NetFlow TCAM and ICAM tables.
• The total available entries and mask, used entries and mask, reserved entries and mask, and entries and mask used percentage for the ACL/QoS TCAM tables. The output displays the available, used, reserved, and used percentage of the labels. The output displays the resource of other hardware resources that are related to the ACL/QoS TCAMs (such as available, used, reserved, and used percentage of the LOU, ANDOR, and ORAND).
• The available, used, reserved, and used percentage for the CPU rate limiters.

The `show platform hardware capacity interface` command displays the following information:
• Tx/Rx drops--Displays the sum of transmit and receive drop counters on each online module (aggregate for all ports) and provides the port number that has the highest drop count on the module.
• Tx/Rx per port buffer size--Summarizes the port-buffer size on a per-module basis for modules where there is a consistent buffer size across the module.

The `show platform hardware capacity monitor` command displays the following SPAN information:
• The maximum local SPAN sessions, maximum RSPAN sessions, maximum ERSSPAN sessions, and maximum service module sessions.
• The local SPAN sessions used/available, RSPAN sessions used/available, ERSSPAN sessions used/available, and service module sessions used/available.

The `show platform hardware capacity multicast` command displays the following information:
• Multicast Replication Mode: ingress and egress IPv4 and IPv6 modes.
• The MET table usage that indicates the total used and the percentage used for each module in the system.
• The bidirectional PIM DF table usage that indicates the total used and the percentage used.
The **show platform hardware capacity** command displays the following information:

- PFC operating mode (PFC Version: PFC3A, PFC3B, unknown, and so forth)
- Supervisor redundancy mode (RPR, RPR+, SSO, none, and so forth)
- Module-specific switching information, including the following information:
  - Part number (WS-SUP720-BASE, WS-X6548-RJ-45, and so forth)
  - Series (supervisor engine, fabric, CEF720, CEF256, dCEF256, or classic)
  - CEF Mode (central CEF, dCEF)

The **show platform hardware capacity vlan** command displays the following VLAN information:

- Total VLANs
- VTP VLANs that are used
- External VLANs that are used
- Internal VLANs that are used
- Free VLANs

### Examples

This example shows how to display CPU capacity and utilization information for the route processor, the switch processor, and the LAN module in the Cisco 7600 series router:

```
Router# show platform hardware capacity cpu

CPU Resources

<table>
<thead>
<tr>
<th>Module</th>
<th>5 seconds</th>
<th>1 minute</th>
<th>5 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 RP</td>
<td>0% / 0%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>1 SP</td>
<td>5% / 0%</td>
<td>5%</td>
<td>4%</td>
</tr>
<tr>
<td>7</td>
<td>69% / 0%</td>
<td>69%</td>
<td>69%</td>
</tr>
<tr>
<td>8</td>
<td>78% / 0%</td>
<td>74%</td>
<td>74%</td>
</tr>
</tbody>
</table>

Processor memory: Module Bytes: Total Used %Used

<table>
<thead>
<tr>
<th>Module</th>
<th>Bytes: Total Used %Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 RP</td>
<td>176730048 51774704 29%</td>
</tr>
<tr>
<td>1 SP</td>
<td>192825092 51978936 27%</td>
</tr>
<tr>
<td>7</td>
<td>195111584 35769704 18%</td>
</tr>
<tr>
<td>8</td>
<td>195111584 35798632 18%</td>
</tr>
</tbody>
</table>

I/O memory: Module Bytes: Total Used %Used

<table>
<thead>
<tr>
<th>Module</th>
<th>Bytes: Total Used %Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 RP</td>
<td>35651584 12226672 34%</td>
</tr>
<tr>
<td>1 SP</td>
<td>35651584 9747952 27%</td>
</tr>
<tr>
<td>7</td>
<td>35651584 9616816 27%</td>
</tr>
<tr>
<td>8</td>
<td>35651584 9616816 27%</td>
</tr>
</tbody>
</table>

Router#
```

This example shows how to display EOBC-related statistics for the route processor, the switch processor, and the DFCs in the Cisco 7600 series router:

```
Router# show platform hardware capacity eobc

EOBC Resources

<table>
<thead>
<tr>
<th>Module</th>
<th>Packets/sec</th>
<th>Total packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 RP</td>
<td>Rx: 61</td>
<td>108982</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Tx: 37</td>
<td>77298</td>
<td>0</td>
</tr>
<tr>
<td>1 SP</td>
<td>Rx: 34</td>
<td>101627</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Tx: 39</td>
<td>11541</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Rx: 5</td>
<td>10358</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Tx: 8</td>
<td>18543</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Rx: 5</td>
<td>12130</td>
<td>0</td>
</tr>
</tbody>
</table>

Router#
```
This example shows how to display the current and peak switching utilization:

Router# show platform hardware capacity fabric

Switch Fabric Resources
Bus utilization: current is 100%, peak was 100% at 12:34 12mar45
Fabric utilization: ingress egress

<table>
<thead>
<tr>
<th>Module</th>
<th>channel</th>
<th>speed</th>
<th>current</th>
<th>peak</th>
<th>current</th>
<th>peak</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>20G</td>
<td>100%</td>
<td>100%</td>
<td>12:34 12mar45</td>
<td>100% 12:34 12mar45</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>20G</td>
<td>12%</td>
<td>80%</td>
<td>12:34 12mar45</td>
<td>12%  80% 12:34 12mar45</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>20G</td>
<td>12%</td>
<td>80%</td>
<td>12:34 12mar45</td>
<td>12%  80% 12:34 12mar45</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>8G</td>
<td>12%</td>
<td>80%</td>
<td>12:34 12mar45</td>
<td>12%  80% 12:34 12mar45</td>
</tr>
</tbody>
</table>

Router#

This example shows how to display information about the total capacity, the bytes used, and the percentage that is used for the Flash/NVRAM resources present in the system:

Router# show platform hardware capacity flash

Flash/NVRAM Resources
Usage: Module Device Bytes: Total Used %Used
1 RP bootflash: 31981568 15688048 49%
1 SP disk0: 128577536 105621504 82%
1 SP sup-bootflash: 31981568 29700644 93%
1 SP const_nvram: 129004 856 1%
1 SP nvram: 391160 22065 6%
7 dfc#7-bootflash: 15204352 616540 4%
8 dfc#8-bootflash: 15204352 0 0%

Router#

This example shows how to display the capacity and utilization of the EARLs present in the system:

Router# show platform hardware capacity forwarding

L2 Forwarding Resources
MAC Table usage: Module Collisions Total Used %Used
6 0 65536 11 1%
VPN CAM usage: Total Used %Used
512 0 0%

L3 Forwarding Resources
FIB TCAM usage: Total Used %Used
72 bits (IPv4, MPLS, EoM) 196608 36 1%
144 bits (IP mcast, IPv6) 32768 7 1%
detail: Protocol Used %Used
IPv4 36 1%
MPLS 0 0%
EoM 0 0%
IPv6 4 1%
IPv4 mcast 3 1%
IPv6 mcast 0 0%

Adjacency usage: Total Used %Used
1048576 175 1%
Forwarding engine load:
Module pps peak-pps peak-time
6 8 1972 02:02:17 UTC Thu Apr 21 2005

Netflow Resources
TCAM utilization: Module Created Failed %Used
6 1 0 0%
ICAM utilization: Module Created Failed %Used
6 0 0 0%

Flowmasks:
Mask# Type Features
IPv4: 0 reserved none
IPv4: 1 Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
IPv4: 2 unused none
IPv4: 3 reserved none
IPv4: 0 reserved none
IPv6: 1 unused none
IPv6: 2 unused none
IPv6: 3 reserved none

CPU Rate Limiters Resources
Rate limiters: Total Used Reserved %Used
Layer 3 9 4 1 44%
Layer 2 4 2 2 50%

ACL/QoS TCAM Resources
Key: ACLen - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
QoSnt - QoS TCAM entries, QOSmsk - QoS TCAM masks, OR - ORAND,
Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
LOUdst - LOU destination, ADJ - ACL adjacency
Module ACLen ACLmsk QoSnt QOSmsk Lbl-in Lbl-eg LOUsrc LOUdst ADJ
6 1% 1% 1% 1% 1% 1% 0% 0% 0% 1%

This example shows how to display the interboard communication resources:

Router# show platform hardware capacity ibc
IBC Resources
Module Packets/sec Total packets Dropped packets
1 RP Rx: 3 5001419 0
Tx: 1 1943884 0

This example shows how to display the interface resources:

Router# show platform hardware capacity interface
Interface drops:
Module Total drops: Tx Rx Highest drop port: Tx Rx
9 0 2 0 48
Interface buffer sizes:
Module Bytes: Tx buffer Rx buffer
1 12345 12345
5 12345 12345

This example shows how to display SPAN information:

Router# show platform hardware capacity monitor
SPAN Resources
Source sessions: 2 maximum, 0 used
Type Used
Local 0
RSpan source 0
ERSpan source 0
Service module 0
Destination sessions: 64 maximum, 0 used
Type Used
RSpan destination 0
ERSpan destination (max 24) 0

This example shows how to display the capacity and utilization of resources for Layer 3 multicast functionality:

Router# show platform hardware capacity
**show platform hardware capacity**

**multicast**
L3 Multicast Resources
- IPv4 replication mode: ingress
- IPv6 replication mode: ingress
- Bi-directional FIM Designated Forwarder Table usage: 4 total, 0 (0%) used
- Replication capability: Module
  - IPv4 egress ingress
  - IPv6 egress ingress
- MET table Entries: Module
  - 5 Total 65526 Used 6 %Used

Router#

This example shows how to display information about the system power capacities and utilizations:

Router# `show platform hardware capacity power`

- Power Resources
  - Power supply redundancy mode: administratively combined
  - System power: 1922W, 0W (0%) inline, 1289W (67%) total allocated
  - Powered devices: 0 total

Router#

This example shows how to display the capacity and utilization of QoS policer resources per EARL in the Cisco 7600 series router:

Router# `show platform hardware capacity qos`

- QoS Policer Resources
  - Aggregate policers: Module
    - 1 Total 1024 Used 102 %Used 10%
    - 5 Total 1024 Used 1 %Used 1%
  - Microflow policer configurations: Module
    - 1 Total 64 Used 32 %Used 50%
    - 5 Total 64 Used 1 %Used 1%

Router#

This example shows how to display information about the key system resources:

Router# `show platform hardware capacity system`

- System Resources
  - PFC operating mode: PFC3BXL
  - Supervisor redundancy mode: administratively rpr-plus, operationally rpr-plus

- Switching Resources: Module
  - 5 WS-SUP720-BASE supervisor CEF
  - 9 WS-X6548-RJ-45 CEF256 CEF

Router#

This example shows how to display VLAN information:

Router# `show platform hardware capacity vlan`

- VLAN Resources
  - VLANs: 4094 total, 10 VTP, 0 extended, 0 internal, 4084 free

Router#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mscf</td>
<td>Displays MSFC information.</td>
</tr>
<tr>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
</tbody>
</table>
**show platform isg**

To display Constellation WAN (CWAN) iEdge Route Processor information, use the `show platform isg` command in privileged EXEC mode.

```
show platform isg {memory|detailed}|msi-all|slot|session-count|{slot-number|all}|uid|{subscriber-session UID|all}|vrf|{vrf-number|all}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Displays memory usage information.</td>
</tr>
<tr>
<td>detailed</td>
<td>Displays detailed memory usage information.</td>
</tr>
<tr>
<td>msi-all</td>
<td>Displays CWAN Multiservice Interface (MSI) information.</td>
</tr>
<tr>
<td>slot</td>
<td>Displays active slot session information.</td>
</tr>
<tr>
<td>session-count</td>
<td>Displays CWAN iEdge session count information.</td>
</tr>
<tr>
<td>slot-number</td>
<td>Slot number.</td>
</tr>
<tr>
<td>all</td>
<td>Displays information about all CWAN iEdge slots.</td>
</tr>
<tr>
<td>uid</td>
<td>Displays CWAN information based on Unique ID.</td>
</tr>
<tr>
<td>subscriber-session UID</td>
<td>Displays CWAN information for a specific ID (1-4294967295).</td>
</tr>
<tr>
<td>all</td>
<td>Displays information for all subscriber session IDs.</td>
</tr>
<tr>
<td>vrf</td>
<td>Displays CWAN iEdge VPN routing and forwarding (VRF) information.</td>
</tr>
<tr>
<td>vrf-number</td>
<td>VRF ID.</td>
</tr>
<tr>
<td>all</td>
<td>Displays information about all CWAN VRFs.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>The <code>memory</code>, <code>session-count</code>, and <code>uid</code> keywords were added.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show platform isg vrf all` command. The field descriptions are self-explanatory.

Router# `show platform isg vrf all`
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
</tbody>
</table>

### show platform oam

To display Operation, Administration, and Maintenance (OAM) information of a platform, use the `show platform oam` command in privileged EXEC mode.

**Syntax Description**

- `link-monitor` Displays link monitoring information.
- `interface type number` (Optional) Displays the interface name and number.
- `loopback` Displays information about the loopback ports.

### Command Modes

- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show platform oam link-monitor interface GigabitEthernet 1/1` command. The fields are self-explanatory.

```bash
Router# show platform oam link-monitor interface GigabitEthernet 1/1

Interface Gi1/1:
  first_poll = 0
  symprd_tlv_sent = 0
  frmpdrd_tlv_sent = 0
  frm_poll_cnt = 1
  frmsec_poll_cnt = 10
  rxcrc_poll_cnt = 1
  txcrc_poll_cnt = 1
  symbol_period_start = 00:00:01.752
  prev_rx_error_frames = 2
  total_rx_error_frames = 0
  error_frame_period_start = 2
  total_frame_period_start = 20
  prev_error_frame_seconds = 0
  total_error_frame_seconds = 0
  prev_rx_crc_error_frames = 0
```
show monitor permit list through show process memory

```
prev_tx_crc_error_frames = 2
total_frm_tlvs = 0
total_frmsec_tlvs = 0
total_symprd_tlvs = 0
total_frmprd_tlvs = 0
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
</tbody>
</table>

### show platform redundancy

To display platform-specific Constellation WAN (CWAN) redundancy information, use the `show platform redundancy` command in privileged EXEC mode.

```
show platform redundancy {atm|ccb slot-number
cpu-number|cwpa-ce3|cwpa-ct3|cwpa-e1|cwpa-stm1|cwpa-t1|frame-relay|hdlc|if-config {slot-number
cpu-number
[bay-number]}}|default-retvals|mlp|multilink-vc|osm-chocx|osm-ct3|ppp|shadowstate|spa-chocx|spa-ct3|switchover
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>atm</td>
<td>Displays CWAN ATM redundancy state information.</td>
</tr>
<tr>
<td>ccp</td>
<td>Displays the CWAN Configuration Control Block (CCB) list.</td>
</tr>
<tr>
<td>slot-number</td>
<td>Slot number.</td>
</tr>
<tr>
<td>cpu-number</td>
<td>CPU number.</td>
</tr>
<tr>
<td>cwpa-ce3</td>
<td>Displays CWAN port adapter (CWPA) Channelized E3 (CE3) redundancy state information.</td>
</tr>
<tr>
<td>cwpa-ct3</td>
<td>Displays CWPA-CT3 redundancy state information.</td>
</tr>
<tr>
<td>cwpa-e1</td>
<td>Displays CWPA-E1 redundancy state information.</td>
</tr>
<tr>
<td>cwpa-stm1</td>
<td>Displays CWPA Synchronous Transport Module level-1 (STM-1) virtual circuit (VC) information.</td>
</tr>
<tr>
<td>cwpa-t1</td>
<td>Displays CWPA-T1 redundancy state information.</td>
</tr>
<tr>
<td>frame-relay</td>
<td>Displays CWAN Frame Relay redundancy state information.</td>
</tr>
<tr>
<td>hdlc</td>
<td>Displays CWAN High-Level Data Link Control (HDLC) redundancy state information.</td>
</tr>
<tr>
<td>if-config</td>
<td>Displays the CWAN IF-configuration list.</td>
</tr>
<tr>
<td>bay-number</td>
<td>(Optional) Shared Port Adapter (SPA) bay number.</td>
</tr>
<tr>
<td>default-retvals</td>
<td>Displays default IF-configuration return values.</td>
</tr>
<tr>
<td>mlp</td>
<td>Displays CWAN Multilink Point-to-Point Protocol (MLP) redundancy state information.</td>
</tr>
<tr>
<td>multilink-vc</td>
<td>Displays CWAN Multilink VC information.</td>
</tr>
</tbody>
</table>
osm-chocx | Displays CWAN Optical Services Module (OSM) Channelized OC-12/OC-3 line card (CHOCX) redundancy state information.
---|---
osm-ct3 | Displays CWAN OSM-CT3 redundancy state information.
---|---
ppp | Displays CWAN PPP redundancy state information.
---|---
shadowstate | Displays the CWAN interface descriptor block (IDB) shadow state.
---|---
spa-chocx | Displays CHOCX SPA VC information.
---|---
spa-ct3 | Displays CT3 SPA VC information.
---|---
switchover | Displays CWAN switchover redundancy information.
---|---

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show platform redundancy` command with the `if-config` keyword. The fields are self-explanatory.

Router# show platform redundancy if-config 4 0

Current number of elements = 0
Current maximum elements = 128
List was grown = 0 times
Number of elements sorted = 0
List errors = 0
List flags = 0x1E
Current element pointer = 0x0
List pointer = 0x50A27438

+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| C=Command T=Type P=Port t=timedOut D=Dirty S=Sync |
| +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| C | T | P | key address | t | D | S | value |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform</td>
<td>Displays platform information.</td>
</tr>
</tbody>
</table>

**show platform software filesystem**

To display information about file systems, use the `show platform software filesystem` command in privileged EXEC or diagnostic mode.
show platform software filesystem

Syntax Description

- **bootflash:** File system on the bootflash device.
- **stby-bootflash:** Standby file system on the bootflash device (if the standby Route Processor [RP] is preset).
- **fpd:** Synthetic file system that is used by the field-programmable device (FPD) upgrade process—for Cisco Technical Support only.
- **harddisk:** File system on the hard disk device.
- **stby-harddisk:** Standby file system on the harddisk device (if the standby RP is preset).
- **obfl:** File system on the on board failure logging (OBFL) device.
- **stby-obfl:** Standby file system on the OBFL device (if the standby RP is preset).
- **usb0:** File system on the USB0 device (if installed).
- **stby-usb0:** Standby file system on the USB0 device (if the standby RP is preset).
- **usb1:** File system on the USB1 device (if installed).
- **stby-usb1:** Standby file system on the USB1 device (if the standby RP is preset).
- **all** (Optional) All possible device information.
- **details** (Optional) File system details.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR1000 Series Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to ascertain the presence or absence of specific files and to determine space usage in the file system. This command is helpful to monitor the growth of log file sizes, because rapid growth of log files could indicate possible problems with the router.

Examples

The following example displays information about the files in the bootflash file system. It also shows the number of bytes used out of the total available in the bootflash file system.

```
Router# show platform software filesystem bootflash:
## --length-- -----------date/time----------- path
1  4096 Apr 01 2008 13:34:30 +00:00 /bootflash/
2  16384 Dec 04 2007 04:32:46 +00:00 /bootflash/lost+found
3  4096 Dec 04 2007 06:06:24 +00:00 /bootflash/.ssh
```
The following example displays information only about the bootflash file system itself, such as file system type and access permissions:

Router# show platform software filesystem bootflash: details
Filesystem: bootflash
Filesystem Path: /bootflash
Filesystem Type: ext2
Mounted: Read/Write

The table below describes the significant fields shown in the displays of file system information.

**Table 139: show platform software filesystem Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Display line number.</td>
</tr>
<tr>
<td>Length</td>
<td>File size in bytes.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time the file system was created.</td>
</tr>
<tr>
<td>Path</td>
<td>Full path of a file in the file system.</td>
</tr>
<tr>
<td>Filesystem Path</td>
<td>Root of the file system.</td>
</tr>
<tr>
<td>Filesystem Type</td>
<td>Type of file system. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• ext2--Second extended file system.</td>
</tr>
<tr>
<td></td>
<td>• jffs2--Journaling file system, version 2.</td>
</tr>
<tr>
<td></td>
<td>• vfat--Virtual file allocation table (FAT16 or FAT32).</td>
</tr>
<tr>
<td>Mounted</td>
<td>Access permissions to the file system.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show platform software mount</strong></td>
<td>Displays the mounted file systems (both physical and virtual) on a shared port adapter (SPA) in a SPA interface processor (SIP), on an Embedded Services Processor (ESP), or on a Route Processor (RP).</td>
</tr>
<tr>
<td><strong>show platform software tech-support</strong></td>
<td>Displays system information or creates a technical support information tar file for Cisco Technical Support.</td>
</tr>
</tbody>
</table>

### show platform software memory

To display memory information for the specified process, use the `show platform software memory` command in privileged EXEC or diagnostic mode.

```
show platform software memory [([database|messaging!])|chassis-manager slot|cpp-control-process process|cpp-driver process|cpp-ha-server process|cpp-service-process process|forwarding-manager slot|host-manager slot|interface-manager slot|ios slot|logger slot|pluggable-services slot|shell-manager slot] [brief]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>database database</td>
<td>(Optional) Displays database memory information for the specified process.</td>
</tr>
<tr>
<td>messaging</td>
<td>(Optional) Displays messaging memory information for specified process. The information displayed is for internal debugging purposes only.</td>
</tr>
</tbody>
</table>
| chassis-manager slot | Displays memory information for the Chassis Manager process in the specified `slot`. Possible `slot` values are:  
  - `0` -- Cisco ASR 1000 Series SPA Interface Processor (SIP) slot 0  
  - `1` -- Cisco ASR 1000 Series SIP slot 1  
  - `2` -- Cisco ASR 1000 Series SIP slot 2  
  - `f0` -- Cisco ASR 1000 Series Embedded Services Processor (ESP) slot 0  
  - `f1` -- Cisco ASR 1000 Series ESP slot 1  
  - `fp active` -- Active Cisco ASR 1000 Series ESP  
  - `fp standby` -- Standby Cisco ASR 1000 Series ESP  
  - `r0` -- Cisco ASR 1000 Series Route Processor (RP) slot 0  
  - `r1` -- Cisco ASR 1000 Series RP slot 1  
  - `rp active` -- Active Cisco ASR 1000 Series RP  
  - `rp standby` -- Standby Cisco ASR 1000 Series RP |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cpp-control-process</strong></td>
<td>Displays memory information for the specified Cisco Packet Processor (CPP) Client Control process. Possible <strong>process</strong> values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp active</strong> --Active CPP Client Control process</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp standby</strong> --Standby CPP Client Control process</td>
</tr>
<tr>
<td></td>
<td>The information displayed is for internal debugging purposes only.</td>
</tr>
<tr>
<td><strong>cpp-driver</strong></td>
<td>Displays memory information for the specified CPP Driver process. Possible <strong>process</strong> values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp active</strong> --Active CPP Driver process</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp standby</strong> --Standby CPP Driver process</td>
</tr>
<tr>
<td></td>
<td>The information displayed is for internal debugging purposes only.</td>
</tr>
<tr>
<td><strong>cpp-ha-server</strong></td>
<td>Displays memory information for the specified CPP High Availability (HA) Server process. Possible <strong>process</strong> values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp active</strong> --Active CPP HA Server process</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp standby</strong> --Standby CPP HA Server process</td>
</tr>
<tr>
<td></td>
<td>The information displayed is for internal debugging purposes only.</td>
</tr>
<tr>
<td><strong>cpp-service-process</strong></td>
<td>Displays memory information for the specified CPP Client Service process. Possible <strong>process</strong> values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp active</strong> --Active CPP Client Service process</td>
</tr>
<tr>
<td></td>
<td>• <strong>cpp standby</strong> --Standby CPP Client Service process</td>
</tr>
<tr>
<td></td>
<td>The information displayed is for internal debugging purposes only.</td>
</tr>
<tr>
<td><strong>forwarding-manager</strong></td>
<td>Displays memory information for the Forwarding Manager process in the specified <strong>slot</strong>. Possible <strong>slot</strong> values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>f0</strong> --Cisco ASR 1000 Series ESP slot 0</td>
</tr>
<tr>
<td></td>
<td>• <strong>f1</strong> --Cisco ASR 1000 Series ESP slot 1</td>
</tr>
<tr>
<td></td>
<td>• <strong>fp active</strong> --Active Cisco ASR 1000 Series ESP</td>
</tr>
<tr>
<td></td>
<td>• <strong>fp standby</strong> --Standby Cisco ASR 1000 Series ESP</td>
</tr>
<tr>
<td></td>
<td>• <strong>r0</strong> --Cisco ASR 1000 Series RP slot 0</td>
</tr>
<tr>
<td></td>
<td>• <strong>r1</strong> --Cisco ASR 1000 Series RP slot 1</td>
</tr>
<tr>
<td></td>
<td>• <strong>rp active</strong> --Active Cisco ASR 1000 Series RP</td>
</tr>
<tr>
<td></td>
<td>• <strong>rp standby</strong> --Standby Cisco ASR 1000 Series RP</td>
</tr>
</tbody>
</table>
| **host-manager** | **slot** | Displays memory information for the Host Manager process in the specified **slot**. Possible **slot** values are:

- **0** -- Cisco ASR 1000 Series SIP slot 0
- **1** -- Cisco ASR 1000 Series SIP slot 1
- **2** -- Cisco ASR 1000 Series SIP slot 2
- **f0** -- Cisco ASR 1000 Series ESP slot 0
- **f1** -- Cisco ASR 1000 Series ESP slot 1
- **fp active** -- Active Cisco ASR 1000 Series ESP
- **fp standby** -- Standby Cisco ASR 1000 Series ESP
- **r0** -- Cisco ASR 1000 Series RP slot 0
- **r1** -- Cisco ASR 1000 Series RP slot 1
- **rp active** -- Active Cisco ASR 1000 Series RP
- **rp standby** -- Standby Cisco ASR 1000 Series RP

| **interface-manager** | **slot** | Displays memory information for the Interface Manager process in the specified **slot**. Possible **slot** values are:

- **0** -- Cisco ASR 1000 Series SIP slot 0
- **1** -- Cisco ASR 1000 Series SIP slot 1
- **2** -- Cisco ASR 1000 Series SIP slot 2
- **r0** -- Cisco ASR 1000 Series RP slot 0
- **r1** -- Cisco ASR 1000 Series RP slot 1
- **rp active** -- Active Cisco ASR 1000 Series RP
- **rp standby** -- Standby Cisco ASR 1000 Series RP

---

Cisco IOS Configuration Fundamentals Command Reference
**display memory information for the IOS process in the specified slot. Possible slot values are:**

- **0/0** -- Cisco ASR 1000 Series SIP slot 0, bay 0
- **0/1** -- Cisco ASR 1000 Series SIP slot 0, bay 1
- **0/2** -- Cisco ASR 1000 Series SIP slot 0, bay 2
- **0/3** -- Cisco ASR 1000 Series SIP slot 0, bay 3
- **1/0** -- Cisco ASR 1000 Series SIP slot 1, bay 0
- **1/1** -- Cisco ASR 1000 Series SIP slot 1, bay 1
- **1/2** -- Cisco ASR 1000 Series SIP slot 1, bay 2
- **1/3** -- Cisco ASR 1000 Series SIP slot 1, bay 3
- **2/0** -- Cisco ASR 1000 Series SIP slot 2, bay 0
- **2/1** -- Cisco ASR 1000 Series SIP slot 2, bay 1
- **2/2** -- Cisco ASR 1000 Series SIP slot 2, bay 2
- **2/3** -- Cisco ASR 1000 Series SIP slot 2, bay 3
- **r0** -- Cisco ASR 1000 Series RP slot 0
- **r1** -- Cisco ASR 1000 Series RP slot 1
- **rp active** -- Active Cisco ASR 1000 Series RP
- **rp standby** -- Standby Cisco ASR 1000 Series RP

**display memory information for the logger process in the specified slot. Possible slot values are:**

- **0** -- Cisco ASR 1000 Series SIP slot 0
- **1** -- Cisco ASR 1000 Series SIP slot 1
- **2** -- Cisco ASR 1000 Series SIP slot 2
- **f0** -- Cisco ASR 1000 Series ESP slot 0
- **f1** -- Cisco ASR 1000 Series ESP slot 1
- **fp active** -- Active Cisco ASR 1000 Series ESP
- **fp standby** -- Standby Cisco ASR 1000 Series ESP
- **r0** -- Cisco ASR 1000 Series RP slot 0
- **r1** -- Cisco ASR 1000 Series RP slot 1
- **rp active** -- Active Cisco ASR 1000 Series RP
- **rp standby** -- Standby Cisco ASR 1000 Series RP
<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
<tr>
<td></td>
<td>Diagnostic (diag)</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>The specification of the database and brief keywords are optional.</td>
</tr>
<tr>
<td></td>
<td>The specification of a process and slot are required.</td>
</tr>
<tr>
<td>Examples</td>
<td></td>
</tr>
<tr>
<td>The following example displays memory information for the Forwarding Manager process for Cisco ASR 1000 Series RP slot 0:</td>
<td></td>
</tr>
</tbody>
</table>

```
Router# show platform software memory forwarding-manager r0
Module: cdllib
  allocated: 900, requested: 892, overhead: 8
  Allocations: 2, failed: 0, frees: 1
Module: eventutil
  allocated: 117379, requested: 117059, overhead: 320
  Allocations: 46, failed: 0, frees: 6
Module: uipeer
  allocated: 9264, requested: 9248, overhead: 16
  Allocations: 3, failed: 0, frees: 1
Module: Summary
  allocated: 127543, requested: 127199, overhead: 344
  Allocations: 51, failed: 0, frees: 8
```

The table below describes the significant fields shown in the display.
### Table 140: show platform software memory Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module:</td>
<td>Name of submodule.</td>
</tr>
<tr>
<td>allocated:</td>
<td>Memory, allocated in bytes.</td>
</tr>
<tr>
<td>requested:</td>
<td>Number of bytes requested by application.</td>
</tr>
<tr>
<td>overhead:</td>
<td>Allocation overhead.</td>
</tr>
<tr>
<td>Allocations:</td>
<td>Number of discrete allocation event attempts.</td>
</tr>
<tr>
<td>failed:</td>
<td>Number of allocation attempts that were attempted, but failed.</td>
</tr>
<tr>
<td>frees:</td>
<td>Number of free events.</td>
</tr>
</tbody>
</table>

The following example displays abbreviated (brief keyword) memory information for the Chassis Manager process for Cisco ASR 1000 Series ESP slot 0:

```
Router# show platform software memory chassis-manager f0 brief
```

<table>
<thead>
<tr>
<th>module</th>
<th>allocated</th>
<th>requested</th>
<th>allocs</th>
<th>frees</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPP Features</td>
<td>692</td>
<td>668</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Summary</td>
<td>497816</td>
<td>495344</td>
<td>323</td>
<td>14</td>
</tr>
<tr>
<td>chunk</td>
<td>419322</td>
<td>419290</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>eventutil</td>
<td>68546</td>
<td>66146</td>
<td>312</td>
<td>12</td>
</tr>
<tr>
<td>uipeer</td>
<td>9256</td>
<td>9240</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

The table below describes the significant fields shown in the `brief` keyword display.

### Table 141: show platform software memory brief Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module</td>
<td>Name of submodule.</td>
</tr>
<tr>
<td>allocated</td>
<td>Memory, allocated in bytes.</td>
</tr>
<tr>
<td>requested</td>
<td>Number of bytes requested by application.</td>
</tr>
<tr>
<td>allocs</td>
<td>Number of discrete allocation event attempts.</td>
</tr>
<tr>
<td>frees</td>
<td>Number of free events.</td>
</tr>
</tbody>
</table>

### show platform software mount

To display the mounted file systems, both physical and virtual, for a Cisco ASR 1000 Series SPA Interface Processor (SIP), Cisco ASR 1000 Series Embedded Services Processor (ESP), or Cisco ASR 1000 Series Route Processor (RP), use the `show platform software mount` command in privileged EXEC or diagnostic mode.
show platform software mount [slot  [brief]]

**Syntax Description**

<table>
<thead>
<tr>
<th>slot</th>
<th>(Optional) Displays mounted file systems for the specified slot. Possible slot values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>--Cisco ASR 1000 Series SIP slot 0</td>
</tr>
<tr>
<td>1</td>
<td>--Cisco ASR 1000 Series SIP slot 1</td>
</tr>
<tr>
<td>2</td>
<td>--Cisco ASR 1000 Series SIP slot 2</td>
</tr>
<tr>
<td>f0</td>
<td>--Cisco ASR 1000 Series ESP slot 0</td>
</tr>
<tr>
<td>f1</td>
<td>--Cisco ASR 1000 Series ESP slot 1</td>
</tr>
<tr>
<td>fp active</td>
<td>--Active Cisco ASR 1000 Series ESP</td>
</tr>
<tr>
<td>fp standby</td>
<td>--Standby Cisco ASR 1000 Series ESP</td>
</tr>
<tr>
<td>r0</td>
<td>--Cisco ASR 1000 Series RP slot 0</td>
</tr>
<tr>
<td>r1</td>
<td>--Cisco ASR 1000 Series RP slot 1</td>
</tr>
<tr>
<td>rp active</td>
<td>--Active Cisco ASR 1000 Series RP</td>
</tr>
<tr>
<td>rp standby</td>
<td>--Standby Cisco ASR 1000 Series RP</td>
</tr>
</tbody>
</table>

| brief      | (Optional) Displays abbreviated mounted file system information. |

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)
Diagnostic (diag)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no slot is specified, the command returns mounted file systems for the active RP.

This command allows you to ascertain the presence or absence of specific system mounts. For example, this command might be used to determine /tmp-related mounts, which are used to create many run-time directories and files.

Users may be requested to execute this command to collect information about the underlying configuration of the platform software.

The RP output can differ depending on how the router was booted, and whether there are USB devices inserted.

The SIP and ESP output can differ depending on whether the chassis is a dual or single RP.

**Examples**

The following example displays mounted file systems for the active RP:

```
Router# show platform software mount
Filesystem  Used  Available  Use% Mounted on
rootfs      0      0           -  /
```
The following example displays mounted file systems for the Cisco ASR 1000 Series ESP in ESP slot 0:

Router# show platform software mount f0

Filesystem Used Available Use% Mounted on
rootfs 0 0 - /
proc 0 0 - /proc
sysfs 0 0 - /sys
none 10864 507124 3% /dev
/dev/loop1 41418 0 100% /tmp/sw/mount/2007-09-27...
none 10864 507124 3% /dev
/procbus/usb 0 0 - /procbus/usb
/dev/mtdblock1 504 1544 25% /obfl
automount(pid3210) 0 0 - /misc1

The following example displays mounted file systems for the active Cisco ASR 1000 Series RP:

Router# show platform software mount rp active

Filesystem Used Available Use% Mounted on
rootfs 0 0 - /
proc 0 0 - /proc
sysfs 0 0 - /sys
none 436 1037728 1% /dev
/dev/bootflash1 256809 83864 76% /bootflash
/dev/harddisk1 252112 4382228 6% /misc/scratch
/dev/loop1 30348 0 100% /tmp/sw/mount/2007-09-27...
/dev/loop2 28394 0 100% /tmp/sw/mount/2007-09-27...
/dev/loop3 42062 0 100% /tmp/sw/mount/2007-09-27...
/dev/loop4 8384 0 100% /tmp/sw/mount/2007-09-27...
/dev/loop5 41418 0 100% /tmp/sw/mount/2007-09-27...
/dev/loop6 21612 0 100% /tmp/sw/mount/2007-09-27...
/dev/loop7 16200 0 100% /tmp/sw/mount/2007-09-27...
none 436 1037728 1% /dev
/procbus/usb 0 0 - /procbus/usb
/dev/mtdblock1 484 1564 24% /obfl
automount(pid4004) 0 0 - /vol

The table below describes the significant fields shown in the SIP slot (0, 1, or 2) displays.

**Table 142: show platform software mount SIP slot Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem</td>
<td>Logical name of the file system device.</td>
</tr>
</tbody>
</table>
The following example displays abbreviated (brief keyword) mounted file system information for Cisco ASR 1000 Series SIP slot 0:

Router# `show platform software mount 0 brief`

<table>
<thead>
<tr>
<th>Mount point: rootfs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : rootfs</td>
</tr>
<tr>
<td>Location : /</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: proc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : proc</td>
</tr>
<tr>
<td>Location : /proc</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: sysfs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : sysfs</td>
</tr>
<tr>
<td>Location : /sys</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : tmpfs</td>
</tr>
<tr>
<td>Location : /dev</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : tmpfs</td>
</tr>
<tr>
<td>Location : /dev</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: /dev/loop1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : iso9660</td>
</tr>
<tr>
<td>Location : /tmp/sw/cc/0/0/cc/mount</td>
</tr>
<tr>
<td>Options : ro</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : tmpfs</td>
</tr>
<tr>
<td>Location : /dev</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: /proc/bus/usb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : usbfs</td>
</tr>
<tr>
<td>Location : /proc/bus/usb</td>
</tr>
<tr>
<td>Options : rw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: /dev/mtdblock1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : jffs2</td>
</tr>
<tr>
<td>Location : /obfl</td>
</tr>
<tr>
<td>Options : rw,noatime,nodiratime</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mount point: automount(pid3199)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type : autofs</td>
</tr>
<tr>
<td>Location : /misc1</td>
</tr>
<tr>
<td>Options : rw,fd=5,pgrp=3199,timeout=60,minproto=2,maxproto=4,indirect</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used</td>
<td>Number of 1Kb blocks used.</td>
</tr>
<tr>
<td>Available</td>
<td>Number of free 1Kb blocks available.</td>
</tr>
<tr>
<td>Use%</td>
<td>Percentage of 1Kb blocks used of the total available.</td>
</tr>
<tr>
<td>Mounted on</td>
<td>Canonical path to the mounted file system.</td>
</tr>
</tbody>
</table>
### show platform software process list

To display a list of the processes running in a given slot, use the `show platform software process list` command in privileged EXEC or diagnostic mode.

**show platform software process list slot [{name process-name} {process-id} {sort memory|summary}]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>slot</th>
<th>Displays running process information for the specified slot. Possible slot values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• 0--Cisco ASR 1000 Series SPA Interface Processor (SIP) slot 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1--Cisco ASR 1000 Series SIP slot 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2--Cisco ASR 1000 Series SIP slot 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• f0--Cisco ASR 1000 Series Embedded Services Processor (ESP) slot 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• f1--Cisco ASR 1000 Series ESP slot 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fp active--Active Cisco ASR 1000 Series ESP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fp standby--Standby Cisco ASR 1000 Series ESP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• r0--Cisco ASR 1000 Series Route Processor (RP) slot 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• r1--Cisco ASR 1000 Series RP slot 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rp active--Active Cisco ASR 1000 Series RP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rp standby--Standby Cisco ASR 1000 Series RP</td>
</tr>
<tr>
<td>name process-name</td>
<td>(Optional)</td>
<td>Displays information for the specified process name.</td>
</tr>
<tr>
<td>process-id</td>
<td>(Optional)</td>
<td>Displays information for the specified process ID.</td>
</tr>
<tr>
<td>sort memory</td>
<td>(Optional)</td>
<td>Sorts the processes by memory.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional)</td>
<td>Displays summary process information for the running host.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.
show monitor permit list through show process memory

show platform software process list

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The name and process-id keywords can be used to narrow the process list display down to specific processes.
The sort keyword can be used to sort the process list by memory size.
The summary keyword can be used to display summary information about running processes.

Examples

The following example displays information about running processes for Cisco ASR 1000 Series SIP slot 0:

Router# show platform software process list 0

Name   Pid   PPid Group Id Status  Priority Size
init    1     0   1     S     20    1974272
ksoftirqd/0 2 1   1     S     39    0
events/0   3 1   1     S     15    0
khelper  4     1  1     S     15    0
kthread   5 1   1     S     15    0
kblockd/0 19 5   1     S     15    0
khubd    23 5   1     S     15    0
pfflush  59     5  1     S     20    0
pfflush  60     5  1     S     20    0
kswapd0  61 5   1     S     15    0
aio/0 62     5  1     S     15    0
xfslolg/0 63 5   1     S     15    0
xfsdatal/0 64 5   1     S     15    0
mtdblockd 626 1   1     S     20    0
loop0 1370 1   1     S     1974272
portmap 1404 1  1404  S     20    2076672
portmap 1406 1  1406  S     20    2076672
loop1 1440 1   1     S     0     0
udev 2104 1   2104  S     16    1974272
jffs2_gcd_mtd1 2796 1  1     S     30    0
klogd 3093 1   3093  S     20    1728512
automount 3199 1  3199  S     20    2396160
xinetd 3214 1   3214  S     20    3026944
xinetd 3216 1   3216  S     20    3026944
pvp.sh 3540 1   3540  S     20    3678208
inotifywait 3575 3540 3575  S     20    1900544
pman.sh 3614 3540 3614  S     20    3571712
pman.sh 3714 3540 3714  S     20    3571712
btrace_rotate.s 3721 3614 3721  S     20    3133440
agetty 3822 1   3822  S     20    1720320
mcp_chvrf.sh 3823 1  3823  S     20    2990080
snmp 3824 1   3824  S     20    2625536
issu_switchover 3825 1  3825  S     20    3899992
xinetd 3827 3823 3823  S     20    3026944
cmcc 3862 3714 3862  S     20    26710016
pman.sh 3883 3540 3883  S     20    3571712
pman.sh 4014 3540 4014  S     20    3575808
hnman 4020 3883 4020  R     20    19615744
imcced 4114 4014 4114  S     20    31539200
The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>Pid</td>
<td>Process ID.</td>
</tr>
<tr>
<td>PPid</td>
<td>Parent Process ID.</td>
</tr>
<tr>
<td>Group Id</td>
<td>Process group ID.</td>
</tr>
<tr>
<td>Status</td>
<td>Process status.</td>
</tr>
<tr>
<td>Priority</td>
<td>Process priority.</td>
</tr>
<tr>
<td>Size</td>
<td>Virtual memory size (in bytes).</td>
</tr>
</tbody>
</table>

The following example displays information about a specific named process for Cisco ASR 1000 Series SIP slot 0:

Router# show platform software process list 0 name sleep
Name: sleep
    Process id  : 25938
    Parent process id: 3891
    Group id : 3891
    Status : S
    Session id : 3816
    User time : 0
    Kernel time : 0
    Priority : 20
    Virtual bytes : 2482176
    Resident pages : 119
    Resident limit : 4294967295
    Minor page faults: 182
    Major page faults: 0

The following example displays information about a specific process identifier for Cisco ASR 1000 Series SIP slot 0:

Router# show platform software process list 0 process-id 1
Name: init
    Process id  : 1
    Parent process id: 0
    Group id : 1
    Status : S
    Session id : 1
    User time : 1
    Kernel time : 741
    Priority : 20
    Virtual bytes : 1974272
    Resident pages : 161
Resident limit : 4294967295
Minor page faults: 756
Major page faults: 0

The table below describes the significant fields shown in the name and process-id keyword displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>Process id</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Parent process id</td>
<td>Parent process ID.</td>
</tr>
<tr>
<td>Group id</td>
<td>Process group ID.</td>
</tr>
<tr>
<td>Status</td>
<td>Process status.</td>
</tr>
<tr>
<td>Session id</td>
<td>Process session ID.</td>
</tr>
<tr>
<td>User time</td>
<td>Time (in seconds) spent in user mode.</td>
</tr>
<tr>
<td>Kernel time</td>
<td>Time (in seconds) spent in kernel mode.</td>
</tr>
<tr>
<td>Priority</td>
<td>Process priority.</td>
</tr>
<tr>
<td>Virtual bytes</td>
<td>Virtual memory size (in bytes).</td>
</tr>
<tr>
<td>Resident pages</td>
<td>Resident page size.</td>
</tr>
<tr>
<td>Resident limit</td>
<td>Current limit on Resident pages.</td>
</tr>
<tr>
<td>Minor page faults</td>
<td>Number of minor page faults.</td>
</tr>
<tr>
<td>Major page faults</td>
<td>Number of major page faults.</td>
</tr>
</tbody>
</table>

The following example displays process summary information for Cisco ASR 1000 Series SIP slot 0:

```
Router# show platform software process list 0 summary
Total number of processes: 54
  Running : 4
  Sleeping : 50
  Disk sleeping : 0
  Zombies : 0
  Stopped : 0
  Paging : 0
  Up time : 1562
  Idle time : 1511
  User time : 1606
  Kernel time : 1319
  Virtual memory : 587894784
  Pages resident : 45436
  Major page faults: 25
  Minor page faults: 149098
  Architecture : ppc
  Memory (kB)
```
The table below describes the significant fields shown in the summary keyword display.

**Table 146: show platform software process list summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of processes</td>
<td>Total number of processes in all possible states.</td>
</tr>
<tr>
<td>Running</td>
<td>Number of processes in the running state.</td>
</tr>
<tr>
<td>Sleeping</td>
<td>Number of processes in the sleeping state.</td>
</tr>
<tr>
<td>Disk sleeping</td>
<td>Number of processes in the disk-sleeping state.</td>
</tr>
<tr>
<td>Zombies</td>
<td>Number of processes in the zombie state.</td>
</tr>
<tr>
<td>Stopped</td>
<td>Number of processes in the stopped state.</td>
</tr>
<tr>
<td>Paging</td>
<td>Number of processes in the paging state.</td>
</tr>
<tr>
<td>Up time</td>
<td>System Up time (in seconds).</td>
</tr>
<tr>
<td>Idle time</td>
<td>System Idle time (in seconds).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User time</td>
<td>System time (in seconds) spent in user mode.</td>
</tr>
<tr>
<td>Kernel time</td>
<td>System time (in seconds) spent in kernel mode.</td>
</tr>
<tr>
<td>Virtual memory</td>
<td>Virtual memory size (in bytes).</td>
</tr>
<tr>
<td>Pages resident</td>
<td>Resident page size.</td>
</tr>
<tr>
<td>Major page faults</td>
<td>Number of major page faults.</td>
</tr>
<tr>
<td>Minor page faults</td>
<td>Number of minor page faults.</td>
</tr>
<tr>
<td>Architecture</td>
<td>System CPU architecture: PowerPC (ppc).</td>
</tr>
<tr>
<td>Memory (kB)</td>
<td>System memory heading.</td>
</tr>
<tr>
<td>Physical</td>
<td>Total physical memory (in kilobytes).</td>
</tr>
<tr>
<td>Total</td>
<td>Total available memory (in kilobytes). This value represents the physical memory available for kernel use.</td>
</tr>
<tr>
<td>Used</td>
<td>Used memory (in kilobytes).</td>
</tr>
<tr>
<td>Free</td>
<td>Free memory (in kilobytes).</td>
</tr>
<tr>
<td>Active</td>
<td>Most recently used memory (in kilobytes).</td>
</tr>
<tr>
<td>Inactive</td>
<td>Memory (in kilobytes) that has been less recently used. It is more eligible to be reclaimed for other purposes.</td>
</tr>
<tr>
<td>Inact-dirty</td>
<td>Memory (in kilobytes) that may need to be written to persistent store (cache or disk).</td>
</tr>
<tr>
<td>Inact-clean</td>
<td>Memory (in kilobytes) that is readily available for re-use.</td>
</tr>
<tr>
<td>Dirty</td>
<td>Memory (in kilobytes) that is waiting to get written back to the disk.</td>
</tr>
<tr>
<td>AnonPages</td>
<td>Memory (in kilobytes) that is allocated when a process requests memory from the kernel via the malloc() system call. This memory has no file backing on disk.</td>
</tr>
<tr>
<td>Bounce</td>
<td>Memory (in kilobytes) that is allocated to bounce buffers.</td>
</tr>
<tr>
<td>Cached</td>
<td>Amount of physical RAM (in kilobytes) used as cache memory.</td>
</tr>
<tr>
<td>Commit Limit</td>
<td>Total amount of memory (in kilobytes) currently available to be allocated on the system. This limit is only adhered to if strict overcommit accounting is enabled.</td>
</tr>
<tr>
<td>Committed As</td>
<td>Total amount of memory (in kilobytes) presently allocated on the system. The committed memory is a sum of all of the memory that has been allocated by processes, even if it has not been used by them as of yet.</td>
</tr>
<tr>
<td>High Total</td>
<td>Total amount of memory (in kilobytes) that is not directly mapped into kernel space. The High Total value can vary based on the type of kernel used.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>High Free</td>
<td>Amount of free memory (in kilobytes) that is not directly mapped into kernel space. The High Free value can vary based on the type of kernel used.</td>
</tr>
<tr>
<td>Low Total</td>
<td>Total amount of memory (in kilobytes) that is directly mapped into kernel space. The Low Total value can vary based on the type of kernel used.</td>
</tr>
<tr>
<td>Low Free</td>
<td>Amount of free memory (in kilobytes) that is directly mapped into kernel space. The Low Free value can vary based on the type of kernel used.</td>
</tr>
<tr>
<td>Mapped</td>
<td>Total amount of memory (in kilobytes) that has been used to map devices, files, or libraries using the mmap command.</td>
</tr>
<tr>
<td>NFS Unstable</td>
<td>Total amount of memory (in kilobytes) used for unstable NFS pages. Unstable NFS pages are pages that have been written into the page cache on the server, but have not yet been synchronized to disk.</td>
</tr>
<tr>
<td>Page Tables</td>
<td>Total amount of memory (in kilobytes) dedicated to the lowest page table level.</td>
</tr>
<tr>
<td>Slab</td>
<td>Total amount of memory (in kilobytes) used by the kernel to cache data structures for its own use.</td>
</tr>
<tr>
<td>VMalloc Chunk</td>
<td>Largest contiguous block of available virtual address space (in kilobytes) that is free.</td>
</tr>
<tr>
<td>VMalloc Total</td>
<td>Total amount of memory (in kilobytes) of total allocated virtual address space.</td>
</tr>
<tr>
<td>VMalloc Used</td>
<td>Total amount of memory (in kilobytes) of used virtual address space.</td>
</tr>
<tr>
<td>Writeback</td>
<td>Memory (in kilobytes) that is actively being written back to the disk.</td>
</tr>
<tr>
<td>Swap (kB)</td>
<td>Swap memory heading.</td>
</tr>
<tr>
<td>Total</td>
<td>Total swap memory (in kilobytes).</td>
</tr>
<tr>
<td>Used</td>
<td>Used swap memory (in kilobytes).</td>
</tr>
<tr>
<td>Free</td>
<td>Free swap memory (in kilobytes).</td>
</tr>
<tr>
<td>Cached</td>
<td>Cached swap memory (in kilobytes).</td>
</tr>
<tr>
<td>Buffers (kB)</td>
<td>Buffers heading.</td>
</tr>
<tr>
<td>Load Average</td>
<td>Indicators of system load.</td>
</tr>
<tr>
<td>1-Min</td>
<td>Average number of processes running for the last minute.</td>
</tr>
<tr>
<td>5-Min</td>
<td>Average number of processes running for the last 5 minutes.</td>
</tr>
<tr>
<td>15-Min</td>
<td>Average number of processes running for the last 15 minutes.</td>
</tr>
</tbody>
</table>

The following example displays process summary information for Cisco ASR 1000 Series sorted by memory size:
<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>PPid</th>
<th>Group Id</th>
<th>Status</th>
<th>Priority</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>linux_iosd-imag</td>
<td>27982</td>
<td>26696</td>
<td>27982</td>
<td>S</td>
<td>20</td>
<td>4294967295</td>
</tr>
<tr>
<td>fman_rp</td>
<td>25857</td>
<td>25309</td>
<td>25857</td>
<td>S</td>
<td>20</td>
<td>684867584</td>
</tr>
<tr>
<td>vman</td>
<td>30685</td>
<td>29587</td>
<td>30685</td>
<td>S</td>
<td>20</td>
<td>194508016</td>
</tr>
<tr>
<td>smand</td>
<td>30494</td>
<td>28948</td>
<td>30494</td>
<td>S</td>
<td>20</td>
<td>103538688</td>
</tr>
<tr>
<td>libvirts</td>
<td>5260</td>
<td>5254</td>
<td>5254</td>
<td>S</td>
<td>20</td>
<td>83197952</td>
</tr>
<tr>
<td>python</td>
<td>10234</td>
<td>10233</td>
<td>10210</td>
<td>S</td>
<td>20</td>
<td>29765632</td>
</tr>
<tr>
<td>python</td>
<td>10975</td>
<td>10234</td>
<td>10975</td>
<td>S</td>
<td>20</td>
<td>29765632</td>
</tr>
<tr>
<td>python</td>
<td>10977</td>
<td>10234</td>
<td>10977</td>
<td>S</td>
<td>20</td>
<td>29765632</td>
</tr>
<tr>
<td>python</td>
<td>10978</td>
<td>10234</td>
<td>10978</td>
<td>S</td>
<td>20</td>
<td>29765632</td>
</tr>
<tr>
<td>python</td>
<td>10979</td>
<td>10234</td>
<td>10979</td>
<td>S</td>
<td>20</td>
<td>29765632</td>
</tr>
<tr>
<td>python</td>
<td>10981</td>
<td>10234</td>
<td>10981</td>
<td>S</td>
<td>20</td>
<td>29765632</td>
</tr>
<tr>
<td>automount</td>
<td>15682</td>
<td>1</td>
<td>15682</td>
<td>S</td>
<td>20</td>
<td>25092096</td>
</tr>
<tr>
<td>cmdand</td>
<td>25530</td>
<td>25309</td>
<td>25530</td>
<td>S</td>
<td>20</td>
<td>23789568</td>
</tr>
<tr>
<td>imand</td>
<td>27198</td>
<td>26090</td>
<td>27198</td>
<td>S</td>
<td>20</td>
<td>22040576</td>
</tr>
<tr>
<td>psd</td>
<td>31284</td>
<td>28535</td>
<td>31284</td>
<td>S</td>
<td>20</td>
<td>16019456</td>
</tr>
<tr>
<td>emd</td>
<td>25712</td>
<td>2417</td>
<td>25712</td>
<td>S</td>
<td>20</td>
<td>15302656</td>
</tr>
<tr>
<td>hman</td>
<td>26622</td>
<td>2517</td>
<td>26622</td>
<td>S</td>
<td>20</td>
<td>14548996</td>
</tr>
<tr>
<td>plogd</td>
<td>28878</td>
<td>27118</td>
<td>28878</td>
<td>S</td>
<td>20</td>
<td>12394440</td>
</tr>
<tr>
<td>btrace_rotate.s</td>
<td>25251</td>
<td>24643</td>
<td>25251</td>
<td>S</td>
<td>20</td>
<td>6008832</td>
</tr>
<tr>
<td>sort_files_by_i</td>
<td>30092</td>
<td>29666</td>
<td>30092</td>
<td>S</td>
<td>20</td>
<td>5234688</td>
</tr>
<tr>
<td>periodic.sh</td>
<td>28469</td>
<td>27490</td>
<td>28469</td>
<td>S</td>
<td>20</td>
<td>2512800</td>
</tr>
<tr>
<td>rotee</td>
<td>5403</td>
<td>1</td>
<td>5403</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>5412</td>
<td>1</td>
<td>5412</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>5438</td>
<td>1</td>
<td>5438</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>5482</td>
<td>1</td>
<td>5482</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>9844</td>
<td>1</td>
<td>9844</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>9958</td>
<td>1</td>
<td>9958</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>16942</td>
<td>1</td>
<td>16942</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>16946</td>
<td>1</td>
<td>16946</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>24383</td>
<td>1</td>
<td>24383</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>24742</td>
<td>1</td>
<td>24742</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>24960</td>
<td>1</td>
<td>24960</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>25107</td>
<td>1</td>
<td>25107</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>25534</td>
<td>1</td>
<td>25534</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>25542</td>
<td>1</td>
<td>25542</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>25880</td>
<td>1</td>
<td>25879</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>26390</td>
<td>1</td>
<td>26390</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>26881</td>
<td>1</td>
<td>26880</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>27728</td>
<td>1</td>
<td>27727</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>27882</td>
<td>1</td>
<td>27881</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>28867</td>
<td>1</td>
<td>28866</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>29220</td>
<td>1</td>
<td>29219</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>29257</td>
<td>1</td>
<td>29256</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>29405</td>
<td>1</td>
<td>29404</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>rotee</td>
<td>29784</td>
<td>1</td>
<td>29783</td>
<td>S</td>
<td>20</td>
<td>4788224</td>
</tr>
<tr>
<td>oom.sh</td>
<td>5560</td>
<td>5246</td>
<td>5560</td>
<td>S</td>
<td>20</td>
<td>4427776</td>
</tr>
<tr>
<td>reflector.sh</td>
<td>15598</td>
<td>1</td>
<td>15598</td>
<td>S</td>
<td>20</td>
<td>3997696</td>
</tr>
<tr>
<td>droputil.sh</td>
<td>15600</td>
<td>1</td>
<td>15600</td>
<td>S</td>
<td>20</td>
<td>3997696</td>
</tr>
<tr>
<td>pvp.sh</td>
<td>24336</td>
<td>1</td>
<td>24335</td>
<td>S</td>
<td>20</td>
<td>3805384</td>
</tr>
<tr>
<td>pman.sh</td>
<td>29066</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3801088</td>
</tr>
<tr>
<td>pman.sh</td>
<td>24643</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3801088</td>
</tr>
<tr>
<td>pman.sh</td>
<td>27490</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3801088</td>
</tr>
<tr>
<td>pman.sh</td>
<td>26696</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3788800</td>
</tr>
<tr>
<td>pman.sh</td>
<td>9679</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
<tr>
<td>pman.sh</td>
<td>9812</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
<tr>
<td>pman.sh</td>
<td>24760</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
<tr>
<td>pman.sh</td>
<td>24917</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
<tr>
<td>pman.sh</td>
<td>25309</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
<tr>
<td>pman.sh</td>
<td>25617</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
<tr>
<td>pman.sh</td>
<td>26090</td>
<td>24336</td>
<td>24335</td>
<td>S</td>
<td>14</td>
<td>3784704</td>
</tr>
</tbody>
</table>
show platform process slot

To monitor the software-running process in a given slot, use the `show platform software process slot` command in privileged EXEC or diagnostic mode.

```
show platform software process slot slot monitor [{cycles cycles}] [{interval delay}] [{lines lines-of-output}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>Specifies the Field Replace Unit (FRU) where the command is run.</td>
</tr>
<tr>
<td>slot</td>
<td>Slot information.</td>
</tr>
<tr>
<td>monitor</td>
<td>Monitors the running processes.</td>
</tr>
<tr>
<td>cycles</td>
<td>Checks the processes multiple times.</td>
</tr>
<tr>
<td>cycles</td>
<td>Number of times the command is run during a single invocation of the command. The range is from 1 to 4294967295. The default is 5.</td>
</tr>
<tr>
<td>interval</td>
<td>Sets delay interval after each command run.</td>
</tr>
</tbody>
</table>
**show platform process slot**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Privileged EXEC (#)</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.1.0S</td>
<td>This command was introduced in a release earlier than Release 3.1.0S on Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample output of the show platform software process slot command. Only 23 lines are displayed because the lines-of-output argument is set to 23:

```plaintext
Router# show platform software process slot 0 monitor cycles 3 interval 2 lines 23
top - 19:29:32 up 1 day, 4:46, 0 users, load average: 0.10, 0.11, 0.09
Tasks: 78 total, 4 running, 74 sleeping, 0 stopped, 0 zombie
Cpu(s): 3.0%us, 2.9%sy, 0.0%ni, 93.9%id, 0.0%wa, 0.1%hi, 0.1%si, 0.0
Mem: 449752k total, 328940k used, 120812k free, 6436k buffers
Swap: 0k total, 0k used, 0k free, 155396k cached
```

**Table 147: show platform software process slot Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%CPU</td>
<td>CPU Usage</td>
</tr>
<tr>
<td>%MEM</td>
<td>Memory Usage</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAND</td>
<td>Command name or command line</td>
</tr>
<tr>
<td>NI</td>
<td>Nice value</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID</td>
</tr>
<tr>
<td>PR</td>
<td>Priority</td>
</tr>
<tr>
<td>RES</td>
<td>Resident memory size (in kb)</td>
</tr>
<tr>
<td>S</td>
<td>Process status</td>
</tr>
<tr>
<td>SHR</td>
<td>Shared memory size (in kb)</td>
</tr>
<tr>
<td>TIME+</td>
<td>Elapsed execution time</td>
</tr>
<tr>
<td>USER</td>
<td>User name</td>
</tr>
<tr>
<td>VIRT</td>
<td>Virtual memory size (in kb)</td>
</tr>
</tbody>
</table>

### show platform software snapshot status

To display the status of a bootflash snapshot action, use the `show platform software snapshot status` command in privilege EXEC mode.

#### show platform software snapshot slot status

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>snapshot</th>
<th>Requests snapshot actions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td></td>
<td>Specifies the hardware slot. Options include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* number --The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you wanted to specify the SIP in SIP slot 2 of the router, enter 2 as the number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* f0 --The ESP in ESP slot 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* f1 --The ESP in ESP slot 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* fp active --The active ESP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* fp standby --The standby ESP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* r0 --The RP in RP slot 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* r1 --The RP in RP slot 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* rp active --The active RP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* rp standby --The standby RP.</td>
</tr>
<tr>
<td>status</td>
<td></td>
<td>Displays the status of snapshot operations.</td>
</tr>
</tbody>
</table>
show platform software tech-support

To display system information or create a technical support information tar file for Cisco Technical Support, use the `show platform software tech-support` command in privileged EXEC or diagnostic mode.

```
show platform software tech-support [file]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>file</code></td>
<td>(Optional) Creates a technical support information tar file for the specified destination file path.</td>
</tr>
<tr>
<td><code>bootflash: filename .tgz</code></td>
<td>Creates a technical support information tar file for the boot flash memory file system on the active RP.</td>
</tr>
<tr>
<td><code>fpd:filename.tgz</code></td>
<td>Creates a technical support information tar file for the field-programmable device (FPD) image package on the active RP. The information displayed is for internal debugging purposes only.</td>
</tr>
<tr>
<td><code>harddisk:filename.tgz</code></td>
<td>Creates a technical support information tar file for the hard disk file system on the active RP.</td>
</tr>
<tr>
<td><code>obfl:filename.tgz</code></td>
<td>Creates a technical support information tar file for the file system for Onboard Failure Logging (obfl) files. The information displayed is for internal debugging purposes only.</td>
</tr>
<tr>
<td><code>stby-bootflash: filename .tgz</code></td>
<td>Creates a technical support information tar file for the boot flash memory file system on the standby RP. The information displayed is for internal debugging purposes only.</td>
</tr>
</tbody>
</table>
**stby-harddisk: filename.tgz**

Creates a technical support information tar file for the hard disk file system on the standby RP. The information displayed is for internal debugging purposes only.

**stby-obfl:filename.tgz**

Creates a technical support information tar file for the Onboard Failure Logging (obfl) files on the standby RP. The information displayed is for internal debugging purposes only.

**stby-usb0:filename.tgz**

Creates a technical support information tar file for Universal Serial Bus (USB) memory. The information displayed is for internal debugging purposes only.

**stby-usb1:filename.tgz**

Creates a technical support information tar file for Universal Serial Bus (USB) memory. The information displayed is for internal debugging purposes only.

---

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

Diagnostic (diag)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the file keyword is specified, the specification of the bootflash: or harddisk: keyword and filename is required.

The show platform software tech-support command without a destination file path specification returns a large volume of information in a short period of time. You should save the output of the show platform software tech-support command in a log file to send to Cisco Technical Support for analysis.

**Examples**

The following example displays system information for Cisco Technical Support:

```
Router# show platform software tech-support
---- show version installed -----  
Type: provisioning file, Version: unknown  
Provisioned on: RP0, Status: active  
File: packages.conf.super  
Modified: 2007-11-07 15:06:12.212303000 +0000  
SHA1 (header): d929d995d5ba2d3dedf67137c3e0e321b1727d7b  
SHA1 (calculated): d929d995d5ba2d3dedf67137c3e0e321b1727d7b  
SHA1 (external): a16881b6a7e3a5593b63f211f72b8af9c534063

instance address : 0X890DE9B4
  fast failover address : 00000000
  cpp interface handle 0

instance address : 0X890DE9BB
  fast failover address : 00000000
  cpp interface handle 0

instance address : 0X890DE9BC
  fast failover address : 00000000
```

---

show monitor permit list through show process memory
The show platform software tech-support command returns a large volume of information in a short period of time. The example above has been abbreviated for the purposes of this description.

The following example creates a technical support information tar file for the boot flash memory file system on the active RP:

Router# show platform software tech-support file bootflash:tech_support_output.tgz
Running tech support command set; please wait...
Creating file 'bootflash:target_support_output.tgz.tgz' ...
File 'bootflash:target_support_output.tgz.tgz' created successfully

The following example creates a technical support information tar file for the hard disk file system on the active RP:

Router# show platform software tech-support file harddisk:tech_support_output.tgz
Running tech support command set; please wait...
Creating file 'harddisk:tech_support_output.tgz.tgz' ...
File 'harddisk:tech_support_output.tgz.tgz' created successfully

show platform subscriber-group

To display the subscriber group information, use the show platform subscriber-group command in privileged EXEC mode.

```
show platform subscriber-group {vrf-number|all} [detail]
```

**Syntax Description**

- **vrf-number**: VRF identification number. Displays VPN routing and forwarding (VRF) information for the specified VRF ID.
- **all**: Displays information about all VRFs.
- **detail**: Displays detailed information about the subscriber group.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

- **Release** | **Modification**
  - 15.1(1)S | This command was introduced.

**Examples**

This is sample output from the show platform subscriber-group all command:

```
Router#show platform subscriber-group all
Container0[:0] No of access sub-if(s) 1
  Vlan 1014 p_cnt 1 Old Vlan 0 ip T
Container2[VRF2:2] No of access sub-if(s) 1
  Vlan 1018 p_cnt 1 Old Vlan 0 ip T
```
This is sample output from the `show platform subscriber-group 0 detail` command:

```
Router# show platform subscriber-group 0 detail
------------------------------------------
VRF[:0] Container0 No of access sub-if(s) 1 Vlan 1014
Access Interfaces:
    GigabitEthernet2/10.2
```

**show platform subscriber-group**

To display platform subscriber information, use the `show platform subscriber-group` command in privileged EXEC mode.

```
show platform subscriber-group mtu slot slot-number port port-number
```

**Syntax Description**

- **mtu** Displays supervisor operating Maximum Transmission Unit (MTU).
- **slot slot-number** Displays information for the specified slot.
- **port port-number** Displays information for the specified port.

**Command Modes**

Privileged EXEC (#)

**Command History**

- **Release 12.2(33)SRA** This command was introduced.

**Examples**

The following is sample output from the `show platform supervisor` command. The fields are self-explanatory.

```
Router# show platform supervisor mtu slot 5 port 1
User configured MTU : 9216
Real Operating MTU : 9236
```

**show power**

To display information about the power status, use the `show power` command in user EXEC or privileged EXEC mode.
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>available</td>
<td>(Optional) Displays the available system power (margin).</td>
</tr>
<tr>
<td>inline</td>
<td>(Optional) Displays the inline power status.</td>
</tr>
<tr>
<td>interface number</td>
<td>(Optional) Specifies the interface type; possible valid values are ethernet, fastethernet, gigabitethernet, tengigabitethernet, null, port-channel, and vlan. See the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td>module number</td>
<td>Displays the power status for a specific module.</td>
</tr>
<tr>
<td>redundancy-mode</td>
<td>(Optional) Displays the power-supply redundancy mode.</td>
</tr>
<tr>
<td>status</td>
<td>(Optional) Displays the power status.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all the FRU types.</td>
</tr>
<tr>
<td>fan-tray fan-tray-number</td>
<td>Displays the power status for the fan tray.</td>
</tr>
<tr>
<td>module slot</td>
<td>Displays the power status for a specific module.</td>
</tr>
<tr>
<td>power-supply pwr-supply-number</td>
<td>Displays the power status for a specific power supply; valid values are 1 and 2.</td>
</tr>
<tr>
<td>total</td>
<td>(Optional) Displays the total power that is available from the power supplies.</td>
</tr>
<tr>
<td>used</td>
<td>(Optional) Displays the total power that is budgeted for powered-on items.</td>
</tr>
</tbody>
</table>

### Command Default

This command has no default settings.

### Command Modes

User EXEC Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17a)SX1</td>
<td>The output was changed to include the total system-power information.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was changed to include information about the inline power status for a specific module.</td>
</tr>
<tr>
<td>12.2(17d)SXBB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXBB.</td>
</tr>
<tr>
<td>12.2(18)SXFB</td>
<td>The output was changed to include information about the high-capacity power supplies.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The `interface-number` argument designates the module and port number. Valid values for `interface-number` depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Valid values for `vlan-id` are from 1 to 4094.

The Inline power field in the `show power` output displays the inline power that is consumed by the modules. For example, this example shows that module 9 has consumed 0.300 A of inline power:

```
Inline power  #    current
module       9    0.300A
```

Examples

This example shows how to display the available system power:

```
Router> show power available
system power available = 20.470A
Router> 
```

This example shows how to display power-supply redundancy mode:

```
Router# show power redundancy-mode
system power redundancy mode = redundant
Router# 
```

This command shows how to display the system-power status:

```
Router> show power
system power redundancy mode = combined
system power total = 3984.12 Watts (94.86 Amps @ 42V)
system power used = 1104.18 Watts (26.29 Amps @ 42V)
system power available = 2879.94 Watts (68.57 Amps @ 42V)

Power-Capacity  PS-Fan Output  Oper
PS  Type        Watts  A @42V  Status  Status  State
-----  ------------------ ------- ------ ------ ------ ----- 
1  WS-CAC-3000W  2830.80 67.40 OK  OK  on  
2  WS-CAC-1300W  1153.32 27.46 OK  OK  on  

Note: PS2 capacity is limited to 2940.00 Watts (70.00 Amps @ 42V) when PS1 is not present

Fan Type        Pwr-Allocated  Oper
Watts  A @42V  Status
-----  ------------------ ------- ------ 
1  FAN-MOD-9  241.50  5.75 OK
2  - - failed

Pwr-Requested Pwr-Allocated  Admin Oper
Slot  Card-Type  Watts  A @42V  Watts  A @42V  State  State
-----  ------------------ ------- ------- ------- ------ ------ 
1  WS-X6K-SUP2-2GE  145.32  3.46  145.32  3.46  on  on
2  - -  145.32  3.46  - -  
3  WS-X6516-GBIC  118.02  2.81  118.02  2.81  on  on
5  WS-C6500-SFM  117.18  2.79  117.18  2.79  on  on
7  WS-X6516A-GBIC  214.20  5.10  - -  on  off (insuff cooling capacity)
```
show power

This example shows how to display the power status for all FRU types:

Router#
show power
status all
FRU-type # current admin state oper
power-supply 1 27.460A on on
module 1 4.300A on on
module 2 4.300A - - (reserved)
module 5 2.690A on on
Router#

This example shows how to display the power status for a specific module:

Router#
show power
status module 1
FRU-type # current admin state oper
module 1 -4.300A on on
Router#

This example shows how to display the power status for a specific power supply:

Router#
show power
status power-supply 1
FRU-type # current admin state oper
power-supply 1 27.460A on on
Router#

This example displays information about the high-capacity power supplies:

Router#
show power
status power-supply 2

<table>
<thead>
<tr>
<th>PS</th>
<th>Type</th>
<th>Power-Capacity</th>
<th>PS-Fan</th>
<th>Output Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watts</td>
<td>A @42V Status</td>
<td>Status State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>---------------</td>
<td>----------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>WS-CAC-6000W</td>
<td>2672.04</td>
<td>63.62</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>WS-CAC-9000W-E</td>
<td>2773.68</td>
<td>66.04</td>
<td>OK</td>
</tr>
</tbody>
</table>
Router#

This example shows how to display the total power that is available from the power supplies:

Router#
show power
total
system power total = 27.460A
Router#

This example shows how to display the total power that is budgeted for powered-on items:

Router#
show power
used
system power used = -6.990A
Router#
This command shows how to display the inline power status on the interfaces:

```
Router# show power inline
Interface Admin Oper Power (mWatt) Device
-------------------- ----- ---------- --------------- -----------
FastEthernet9/1 auto on 6300 Cisco 6500 IP Phone
FastEthernet9/2 auto on 6300 Cisco 6500 IP Phone
```

This command shows how to display the inline power status for a specific module:

```
Router# show power inline mod 7
Interface Admin Oper Power (Watts) Device Class
-------------------- ----- ---------- ------- -------------- -----------
Gi7/1 auto on 6.3 Cisco IP Phone 7960 n/a
Gi7/2 static power-deny 0 Ieee PD 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>power enable</td>
<td>Turns on power for the modules.</td>
</tr>
<tr>
<td>power redundancy-mode</td>
<td>Sets the power-supply redundancy mode.</td>
</tr>
</tbody>
</table>

**show processes**

To display information about the active Cisco IOS, Cisco IOS XE, or the Cisco IOS Software Modularity POSIX-style processes, use the `show processes` command in user EXEC or privileged EXEC mode.

```
Cisco IOS Software
show processes [{heapcheck|history|process-id|timercheck}]
```

**Cisco IOS Software Modularity Images and Cisco Catalyst 4500e Series Switches Running Cisco IOS XE Software**

```
show processes
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heapcheck</td>
<td>(Optional) Displays the scheduler heapcheck configuration.</td>
</tr>
<tr>
<td>history</td>
<td>(Optional) For Cisco IOS processes only. Displays the process history in an ordered format.</td>
</tr>
<tr>
<td>process-id</td>
<td>(Optional) For Cisco IOS processes only. An integer that specifies the process for which memory and CPU utilization data will be returned.</td>
</tr>
<tr>
<td>timercheck</td>
<td>(Optional) For Cisco IOS processes only. Displays the processes configured for a timer check.</td>
</tr>
</tbody>
</table>
Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was modified. The <strong>history</strong> keyword was added.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>This command was modified. The <strong>process-id</strong> argument was added.</td>
</tr>
<tr>
<td>12.2(18)SXFT</td>
<td>This command was modified. The syntax was modified to support Cisco IOS Software Modularity images.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was modified. The <strong>timercheck</strong> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1.0.SG</td>
<td>This command was introduced on the Cisco Catalyst 4500e Series Switches.</td>
</tr>
<tr>
<td>15.1(2)S</td>
<td>This command was integrated into Cisco IOS Release 15.1(2)S.</td>
</tr>
<tr>
<td>15.2(1)T</td>
<td>The <strong>heapcheck</strong> keyword was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Cisco IOS Software Modularity

Although no optional keywords or arguments are supported for the base **show processes** command when a Software Modularity image is running, more details about processes are displayed using the **show processes cpu**, **show processes detailed**, **show processes kernel**, and **show processes memory** commands.

Cisco IOS Software

The following example shows how to display the scheduler heapcheck configuration using the **show process heapcheck** command.

**Router# show processes heapcheck**
Scheduler Heapcheck Enabled : N
Scheduler Heapcheck Active : N

The following is sample output from the **show processes** command:

<table>
<thead>
<tr>
<th>PID QTY</th>
<th>PC Runtime (ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>Stacks</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cwe</td>
<td>606E9FCC</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>5600/6000</td>
<td>0 Chunk Manager</td>
</tr>
<tr>
<td>2 Csp</td>
<td>607180F0</td>
<td>0</td>
<td>121055</td>
<td>0</td>
<td>2608/3000</td>
<td>0 Load Meter</td>
</tr>
<tr>
<td>3 M*</td>
<td>0</td>
<td>8</td>
<td>90</td>
<td>88</td>
<td>9772/12000</td>
<td>0 Exec</td>
</tr>
<tr>
<td>4 Mwe</td>
<td>619CB674</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>23512/24000</td>
<td>0 EDDRI_MAIN</td>
</tr>
<tr>
<td>5 Mst</td>
<td>606F6AAA4</td>
<td>82064</td>
<td>61496</td>
<td>1334</td>
<td>5668/6000</td>
<td>0 Check heaps</td>
</tr>
<tr>
<td>6 Cwe</td>
<td>606FD444</td>
<td>0</td>
<td>127</td>
<td>0</td>
<td>5588/6000</td>
<td>0 Pool Manager</td>
</tr>
<tr>
<td>7 Lwe</td>
<td>606BB364</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>5764/6000</td>
<td>0 AAA_SERVER_DEADT</td>
</tr>
<tr>
<td>8 Mst</td>
<td>6063212C</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5564/6000</td>
<td>0 Timers</td>
</tr>
<tr>
<td>9 Mwe</td>
<td>600109D4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5560/6000</td>
<td>0 Serial Background</td>
</tr>
<tr>
<td>10 Mwe</td>
<td>60234848</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5564/6000</td>
<td>0 ATM Idle Timer</td>
</tr>
<tr>
<td>11 Mwe</td>
<td>602B75F0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8564/9000</td>
<td>0 ATM AutoVC Perio</td>
</tr>
<tr>
<td>12 Mwe</td>
<td>602B7054</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5560/6000</td>
<td>0 ATM VC Auto Crea</td>
</tr>
</tbody>
</table>
show monitor permit list through show process memory

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

### Table 148: `show processes` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization for five seconds</td>
<td>CPU utilization for the last 5 seconds. The second number indicates the percentage of CPU time spent at the interrupt level.</td>
</tr>
<tr>
<td>one minute</td>
<td>CPU utilization for the last minute.</td>
</tr>
<tr>
<td>five minutes</td>
<td>CPU utilization for the last 5 minutes.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Q</td>
<td>Process queue priority. Possible values: C (critical), H (high), M (medium), and L (low).</td>
</tr>
<tr>
<td>Ty</td>
<td>Scheduler test. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• * (currently running)</td>
</tr>
<tr>
<td></td>
<td>• E (waiting for an event)</td>
</tr>
<tr>
<td></td>
<td>• S (ready to run, voluntarily relinquished processor)</td>
</tr>
<tr>
<td></td>
<td>• rd (ready to run, wakeup conditions have occurred)</td>
</tr>
<tr>
<td></td>
<td>• we (waiting for an event)</td>
</tr>
<tr>
<td></td>
<td>• sa (sleeping until an absolute time)</td>
</tr>
<tr>
<td></td>
<td>• si (sleeping for a time interval)</td>
</tr>
<tr>
<td></td>
<td>• sp (sleeping for a time interval as an alternate call)</td>
</tr>
<tr>
<td></td>
<td>• st (sleeping until a timer expires)</td>
</tr>
<tr>
<td></td>
<td>• hg (hung: the process will never execute again)</td>
</tr>
<tr>
<td></td>
<td>• xx (dead: the process has terminated, but has not yet been deleted)</td>
</tr>
<tr>
<td>PC</td>
<td>Current program counter.</td>
</tr>
<tr>
<td>Runtime (ms)</td>
<td>CPU time that the process has used (in milliseconds).</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process has been invoked.</td>
</tr>
<tr>
<td>uSecs</td>
<td>Microseconds of CPU time for each process invocation.</td>
</tr>
<tr>
<td>Stacks</td>
<td>Low water mark/Total stack space available (in bytes).</td>
</tr>
</tbody>
</table>
Because platforms have a 4- to 8-millisecond clock resolution, run times are considered reliable only after a large number of invocations or a reasonable, measured run time.

For a list of process descriptions, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_tech_note09186a00800a65d0.shtml.

The following is sample output from the `show processes history` command:

```
Router# show processes history

PID Exectime(ms) Caller PC Process Name
 3   12  0x0 Exec
 16   0  0x603F4DEC GraphIt
 21   0  0x603CFEF4 TTY Background
 22   0  0x6042FD7C Per-Second Jobs
 67   0  0x6015CD38 SMT input
 39   0  0x60178804 FBM Timer
 16   0  0x603F4DEC GraphIt
 21   0  0x603CFEF4 TTY Background
 22   0  0x6042FD7C Per-Second Jobs
 67   0  0x6015CD38 SMT input
 39   0  0x60178804 FBM Timer
 24   0  0x60425070 Compute load avgs
 11   0  0x605210A8 ARP Input
 69   0  0x605FDADF4 DHCPD Database
 69   0  0x605FD568 DHCPD Database
 51   0  0x60670B3C IP Cache Ager
 69   0  0x605FD568 DHCPD Database
 36   0  0x606E956DC SSS Test Client
 69   0  0x605FD568 DHCPD Database
--More--
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Exectime (ms)</td>
<td>Execution time (in milliseconds) of the most recent run or the total execution time of the most recent consecutive runs.</td>
</tr>
<tr>
<td>Caller PC</td>
<td>Current program counter of this process before it was suspended.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Name of the process.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show processes process-id` command:

```plaintext
Router# show processes 6

Process ID 6 [Pool Manager], TTY 0
Memory usage [in bytes]
  Holding: 921148, Maximum: 940024, Allocated: 84431264, Freed: 99432136
  Getbufs: 0, Retbufs: 0, Stack: 12345/67890
CPU usage
  PC: 0x60887600, Invoked: 188, Giveups: 100, uSec: 24
  5Sec: 3.03%, 1Min: 2.98%, 5Min: 1.55%, Average: 0.58%,
  Age: 662314 msec, Runtime: 3841 msec
State: Running, Priority: Normal
```

The table below describes the fields shown in the display.

**Table 150: show processes process-id Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID</td>
<td>Process ID number and process name.</td>
</tr>
<tr>
<td>TTY</td>
<td>Terminal that controls the process.</td>
</tr>
<tr>
<td>Memory usage</td>
<td>This section contains fields that show the memory used by the specified process.</td>
</tr>
<tr>
<td>Holding</td>
<td>Amount of memory currently allocated to the process.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Maximum amount of memory allocated to the process since its invocation.</td>
</tr>
<tr>
<td>Allocated</td>
<td>Bytes of memory allocated by the process.</td>
</tr>
<tr>
<td>Freed</td>
<td>Bytes of memory freed by the process.</td>
</tr>
<tr>
<td>Getbufs</td>
<td>Number of times that the process has requested a packet buffer.</td>
</tr>
<tr>
<td>Retbufs</td>
<td>Number of times that the process has relinquished a packet buffer.</td>
</tr>
<tr>
<td>Stack</td>
<td>Low water mark/Total stack space available (in bytes).</td>
</tr>
<tr>
<td>CPU usage</td>
<td>This section contains fields that show the CPU resources used by the specified process.</td>
</tr>
<tr>
<td>PC</td>
<td>Current program counter of this process before it was suspended.</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process executed since its invocation.</td>
</tr>
<tr>
<td>Giveups</td>
<td>Number of times that the process voluntarily gave up the CPU.</td>
</tr>
<tr>
<td>uSec</td>
<td>Microseconds of CPU time for each process invocation.</td>
</tr>
<tr>
<td>5Sec</td>
<td>CPU utilization by process in the last five seconds.</td>
</tr>
<tr>
<td>1Min</td>
<td>CPU utilization by process in the last minute.</td>
</tr>
<tr>
<td>5Min</td>
<td>CPU utilization by process in the last five minutes.</td>
</tr>
<tr>
<td>Average</td>
<td>The average amount of CPU utilization by the process since its invocation.</td>
</tr>
</tbody>
</table>
Cisco IOS Software Modularity

The following is sample output from the `show processes` command when a Cisco IOS Software Modularity image is running:

```
Router# show processes
Total CPU utilization for 5 seconds: 99.7%; 1 minute: 98.9%; 5 minutes: 86.5%
PID  TID  Prio  STATE  Blocked  Stack   CPU  Name
1    1    0     Ready   0        (128K)  2m28s  procnoto-cisco
1    2    63    Receive 1        0    (128K)  0.000  procnoto-cisco
1    3    10    Receive 1        0    (128K)  0.000  procnoto-cisco
1    4    11    Receive 1        0    (128K)  1.848  procnoto-cisco
1    5    63    Receive 1        0    (128K)  0.000  procnoto-cisco
1    6    63    Receive 1        0    (128K)  0.000  procnoto-cisco
12290 1  10    Receive 1        12288(128K) 0.080  chkptd.proc
12290 2 10    Receive 8        12288(128K) 0.000  chkptd.proc
3    1    15   Condvar 1027388 12288(128K) 0.016  qdelogger
3    2    15   Receive 1        12288(128K) 0.004  qdelogger
3    3    16   Condvar 1040024 12288(128K) 0.004  qdelogger
4    1    10   Receive 1        4096 (128K) 0.016  devc-pty
6    1    62   Receive 1        8192 (128K) 0.256  devcser2681
6    2    63   Intr     8192 (128K) 0.663  devcser2681
7    1    10   Receive 1        32768(128K) 0.080  dumper.proc
7    2    10   Receive 1        32768(128K) 0.008  dumper.proc
7    3    10   Receive 1        32768(128K) 0.000  dumper.proc
7    4    10   Receive 1        32768(128K) 0.020  dumper.proc
7    5    10   Receive 1        32768(128K) 0.008  dumper.proc
4104 2 10   Receive 1        12288(128K) 0.000  pipe
4104 3 10   Receive 1        12288(128K) 0.000  pipe
```

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

### Table 151: `show processes` (Software Modularity) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>TID</td>
<td>Task ID.</td>
</tr>
<tr>
<td>Prio</td>
<td>Process priority.</td>
</tr>
<tr>
<td>STATE</td>
<td>Current state of the process.</td>
</tr>
<tr>
<td>Blocked</td>
<td>Thread (with given process ID) that is currently blocked by the process.</td>
</tr>
</tbody>
</table>
Cisco Catalyst 4500e Series Switches Running Cisco IOS XE software

The following is sample output from the `show processes` command:

```
Switch# show processes
CPU utilization for five seconds: 1%; one minute: 4%; five minutes: 3%

PID    TID  Runtime(ms) Invoked uSecs Stacks Process
1      935  596       156971 84/8192 init
2      0    79       10405 0/8192 kthreadd
3      12   2206     5578  0/8192 migration/0
4      12   772      15601 0/8192 ksoftirqd/0
5      6    1089     6357  0/8192 migration/1
6      14   877      16484 8/8192 ksoftirqd/1
7      15   374      42475 0/8192 events/0
8      9    333      27531 0/8192 events/1
9      5    637      9070  0/8192 khelper
61     28   45       628533 0/8192 kblockd/0
62     80   175     461994 0/8192 kblockd/1
75     0    21      1238  0/8192 khubd
78     0    23       652  0/8192 kseriod
83     7    26      271115 0/8192 kmmcd
120    0    25       320  0/8192 pdflush
121    12   68       190382 0/8192 pdflush
122    0    29       172  0/8192 kswapd0
123    0    31       161  0/8192 aio/0
124    0    33       121  0/8192 aio/1
291    0    35       142  0/8192 kpsmoused
309    0    37       135  0/8192 rpciod/0
310    0    39       128  0/8192 rpciod/1
354    71   425     167583 8/8192 udevd
700    117  3257     35991 0/8192 loop1
716    0    55       1145 0/8192 loop2
732    115  2336     49574 0/8192 loop3
2203   86   627     138015 8/8192 dbus-daemon
2539   0    432      1974 8/8192 portmap
2545   0    434      2011 8/8192 portmap
2588   1    450      2384 8/8192 sshd
2602   2    444      6677 0/8192 xinetd
2606   1    444      3191 8/8192 xinetd
3757   0    71       70   8/8192 vsi work/0
```

--More--

The table below describes the significant fields shown in the display.
Table 152: show processes (Software Modularity) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization for five seconds</td>
<td>CPU utilization for the last 5 seconds. The 3% indicates the percentage of CPU time spent at the interrupt level.</td>
</tr>
<tr>
<td>CPU utilization for one minute</td>
<td>CPU utilization for the last minute.</td>
</tr>
<tr>
<td>CPU utilization for five minutes</td>
<td>CPU utilization for the last 5 minutes.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>TID</td>
<td>Thread ID.</td>
</tr>
<tr>
<td>Runtime(ms)</td>
<td>CPU time that the process has used (in milliseconds).</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process has been invoked.</td>
</tr>
<tr>
<td>uSecs</td>
<td>Microseconds of CPU time for each process invocation.</td>
</tr>
<tr>
<td>Stacks</td>
<td>Size, in kilobytes, of the memory stack.</td>
</tr>
<tr>
<td>Process</td>
<td>Process name.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes cpu</td>
<td>Displays detailed CPU utilization statistics (CPU use per process) when a Software Modularity image is running.</td>
</tr>
<tr>
<td>show processes detailed</td>
<td>Displays detailed information about POSIX and Cisco IOS processes when a Software Modularity image is running.</td>
</tr>
<tr>
<td>show processes kernel</td>
<td>Displays information about System Manager kernel processes when a Software Modularity image is running.</td>
</tr>
<tr>
<td>show processes memory</td>
<td>Displays the amount of system memory used per system process.</td>
</tr>
</tbody>
</table>

show processes cpu

To display detailed CPU utilization statistics (CPU use per process) when Cisco IOS, Cisco IOS XE, or Cisco IOS Software Modularity images are running, use the `show processes cpu` command in user EXEC or privileged EXEC mode.

Cisco IOS Software

`show processes cpu [\{history |table|sorted [\{1min|5min|5sec\}\}]]`

Cisco IOS Software Modularity

`show processes cpu [\{detailed [\{process-id\|process-name\}\]}\|history\}]`
Cisco Catalyst 4500e Series Switches running IOS XE software

show processes cpu [{detailed process [{process-id}process-name]}]|history [{detailed|summary|table}][|sorted}]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>(Optional) Displays CPU history in a graph format.</td>
</tr>
<tr>
<td>table</td>
<td>(Optional) Displays CPU history in a table format.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of the CPU history.</td>
</tr>
<tr>
<td>sorted</td>
<td>(Optional) Displays CPU utilization sorted by percentage.</td>
</tr>
<tr>
<td>1min</td>
<td>(Optional) Sorts CPU utilization based on 1 minute utilization.</td>
</tr>
<tr>
<td>5min</td>
<td>(Optional) Sorts CPU utilization based on 5 minutes utilization.</td>
</tr>
<tr>
<td>5sec</td>
<td>(Optional) Sorts CPU utilization based on 5 seconds utilization.</td>
</tr>
<tr>
<td>detailed</td>
<td>(Optional) Displays more detailed information about Cisco IOS processes (not for POSIX processes).</td>
</tr>
<tr>
<td>process-id</td>
<td>(Optional) Process identifier.</td>
</tr>
<tr>
<td>process-name</td>
<td>(Optional) Process name.</td>
</tr>
</tbody>
</table>

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was modified. The history keyword was added.</td>
</tr>
<tr>
<td>12.3(8)</td>
<td>This command was enhanced to display Address Resolution Protocol (ARP) output.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was enhanced to display ARP output.</td>
</tr>
<tr>
<td>12.2(18)SXF4</td>
<td>This command was enhanced to support Cisco IOS Software Modularity images.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.2(33)SCB3</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SCB3.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The output was modified to display the CPU time in microseconds that the process has used.</td>
</tr>
</tbody>
</table>
If you use the optional history keyword, three graphs are displayed for Cisco IOS images:

- CPU utilization for the last 60 seconds
- CPU utilization for the last 60 minutes
- CPU utilization for the last 72 hours

Maximum usage is measured and recorded every second; average usage is calculated on periods of more than one second. Consistently high CPU utilization over an extended period indicates a problem. Use the show processes cpu command to troubleshoot. Also, you can use the output of this command in the Cisco Output Interpreter tool to display potential issues and fixes. Output Interpreter is available to registered users of Cisco.com who are logged in and have JavaScript enabled.


Cisco IOS Software Modularity

Cisco IOS Software Modularity images display only one graph that shows the CPU utilization for the last 60 minutes. The horizontal axis shows times (for example, 0, 5, 10, 15 minutes), and the vertical axis shows total percentage of CPU utilization (0 to 100 percent).

Cisco IOS Software

The following is sample output from the show processes cpu command without keywords:
The following is sample output from the show processes cpu command on a Cisco uBR10012 router:

```
Router# show processes cpu
CPU utilization for five seconds: 2%/0%; one minute: 2%; five minutes: 2%

PID Runtime(us) Invoked uSecs 5Sec 1Min 5Min TTY Process
1  8 471 16 0.00% 0.00% 0.00% 0 Chunk Manager
2  4 472 8 0.00% 0.00% 0.00% 0 Load Meter
3  0  1 0 0.00% 0.00% 0.00% 0 IPC 0x50000 Vers
4  0 10 0 0.00% 0.00% 0.00% 0 C10K Card Event
5  0 65 0 0.00% 0.00% 0.00% 0 Retransmission o
6  0  5 0 0.00% 0.00% 0.00% 0 IPC ISSU Dispatc
7 5112 472 10830 0.63% 0.18% 0.18% 0 Check heaps
8  0  1 0 0.00% 0.00% 0.00% 0 Pool Manager
9  0  2 0 0.00% 0.00% 0.00% 0 Timers
10 0  2 0 0.00% 0.00% 0.00% 0 Serial Background
11 0 786 0 0.00% 0.00% 0.00% 0 WBCHMTS process
12 0  1 0 0.00% 0.00% 0.00% 0 AAA_SERVER_DEADT
13 0  1 0 0.00% 0.00% 0.00% 0 Policy Manager
14 0  1 0 0.00% 0.00% 0.00% 0 Crash writer
15 0  1 0 0.00% 0.00% 0.00% 0 RO Notify Timers
16 0  1 0 0.00% 0.00% 0.00% 0 RMI RM Notify Wa
17 0 2364 0 0.00% 0.00% 0.00% 0 Facility Alarm
18 0  1 0 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
```

The following is sample output from the show processes cpu command that shows an ARP probe process:

```
Router# show processes cpu | include ARP
```
The following is sample output from the show processes cpu command on a Cisco 4400 Series ISR:

The table below describes the fields shown in the output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization for five seconds</td>
<td>CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.</td>
</tr>
<tr>
<td>one minutes</td>
<td>CPU utilization for the last minute.</td>
</tr>
<tr>
<td>five minutes</td>
<td>CPU utilization for the last 5 minutes.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Runtime (us)</td>
<td>CPU time that the process has used (in microseconds).</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process has been invoked.</td>
</tr>
<tr>
<td>uSecs</td>
<td>Microseconds of CPU time for each process invocation.</td>
</tr>
<tr>
<td>5Sec</td>
<td>CPU utilization by task in the last 5 seconds.</td>
</tr>
<tr>
<td>1Min</td>
<td>CPU utilization by task in the last minute.</td>
</tr>
<tr>
<td>5Min</td>
<td>CPU utilization by task in the last 5 minutes.</td>
</tr>
<tr>
<td>TTY</td>
<td>Terminal that controls the process.</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the process.</td>
</tr>
</tbody>
</table>

Because platforms have a 4- to 8-microsecond clock resolution, run times are considered reliable only after several invocations or a reasonable, measured run time.

Cisco IOS Software Modularity

The following is sample output from the show processes cpu command when a Software Modularity image is running:

Router# show processes cpu
Total CPU utilization for 5 seconds: 99.6%; 1 minute: 98.5%; 5 minutes: 85.3%

<table>
<thead>
<tr>
<th>PID</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0%</td>
<td>0.1%</td>
<td>0.8%</td>
<td>kernel</td>
</tr>
<tr>
<td>3</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>qdelogger</td>
</tr>
</tbody>
</table>
The table below describes the significant fields shown in the display.

**Table 154: show processes cpu (Software Modularity) Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total CPU utilization for five seconds</td>
<td>Total CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.</td>
</tr>
<tr>
<td>1 minute</td>
<td>CPU utilization for the last minute.</td>
</tr>
<tr>
<td>5 minutes</td>
<td>CPU utilization for the last 5 minutes.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>5Sec</td>
<td>Percentage of CPU time spent at the interrupt level for this process during the last five seconds.</td>
</tr>
<tr>
<td>1Min</td>
<td>Percentage of CPU time spent at the interrupt level for this process during the last minute.</td>
</tr>
<tr>
<td>5Min</td>
<td>Percentage of CPU time spent at the interrupt level for this process during the last five minutes.</td>
</tr>
<tr>
<td>Process</td>
<td>Process name.</td>
</tr>
</tbody>
</table>

The following is partial sample output from the `show processes cpu` command with the `detailed` keyword when a Software Modularity image is running:

```
Router# show processes cpu detailed
Total CPU utilization for 5 seconds: 99.6%; 1 minute: 99.3%; 5 minutes: 88.6%
PID/TID  5Sec  1Min  5Min Process Prio  STATE  CPU
1 0.0% 0.7% 0.7% kernel 8.900
   1 0.4% 0.7% 11.4% [idle thread] 0 Ready 2m28s
2 0.0% 0.0% 0.0% 63 Receive 0.000
3 0.0% 0.0% 0.0% 10 Receive 0.000
4 0.0% 0.0% 0.1% 63 Receive 1.848
5 0.0% 0.0% 0.0% 63 Receive 0.000
```

Cisco IOS Configuration Fundamentals Command Reference
### Process Display

<table>
<thead>
<tr>
<th>PID/TID</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
<th>Prio</th>
<th>STATE</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>8214</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>sysmgr.proc</td>
<td>10</td>
<td>Receive</td>
<td>0.216</td>
</tr>
<tr>
<td>1</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.152</td>
</tr>
<tr>
<td>2</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Sigwaitin</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>3</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>4</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>5</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>6</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>7</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>8</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>9</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>10</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>11</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>12</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>13</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.028</td>
</tr>
<tr>
<td>14</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.040</td>
</tr>
<tr>
<td>15</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>16</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>17</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.004</td>
</tr>
<tr>
<td>18</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>19</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>20</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>21</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.004</td>
</tr>
<tr>
<td>22</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PID/TID</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
<th>Prio</th>
<th>STATE</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>8215</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>kosh.proc</td>
<td>10</td>
<td>Reply</td>
<td>0.044</td>
</tr>
<tr>
<td>1</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Reply</td>
<td></td>
<td></td>
<td>0.044</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PID/TID</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
<th>Prio</th>
<th>STATE</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>12290</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>chkptd.proc</td>
<td>10</td>
<td>Receive</td>
<td>0.080</td>
</tr>
<tr>
<td>1</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.080</td>
</tr>
<tr>
<td>2</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PID/TID</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
<th>Prio</th>
<th>STATE</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>12312</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>sysmgr.proc</td>
<td>10</td>
<td>Receive</td>
<td>0.112</td>
</tr>
<tr>
<td>1</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.112</td>
</tr>
<tr>
<td>2</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Sigwaitin</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PID/TID</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
<th>Prio</th>
<th>STATE</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>12316</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>installer.proc</td>
<td>10</td>
<td>Receive</td>
<td>0.072</td>
</tr>
<tr>
<td>1</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>3</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Nanosleep</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>4</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Sigwaitin</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>6</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>10 Receive</td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
</tbody>
</table>

Process sbin/ios-base, type IOS, PID = 12317

CPU utilization for five seconds: 12%/9%; one minute: 13%; five minutes: 10%

<table>
<thead>
<tr>
<th>Task</th>
<th>Runtime(us)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Task Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>219</td>
<td></td>
<td>1503</td>
<td>145</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Hot Service Task</td>
</tr>
<tr>
<td>2</td>
<td>23680</td>
<td></td>
<td>42384</td>
<td>558</td>
<td>2.39%</td>
<td>6.72%</td>
<td>4.81%</td>
<td>Service Task</td>
</tr>
<tr>
<td>3</td>
<td>6104</td>
<td></td>
<td>11902</td>
<td>512</td>
<td>3.51%</td>
<td>1.99%</td>
<td>1.23%</td>
<td>Service Task</td>
</tr>
<tr>
<td>4</td>
<td>1720</td>
<td></td>
<td>5761</td>
<td>298</td>
<td>1.91%</td>
<td>0.90%</td>
<td>0.39%</td>
<td>Service Task</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td></td>
<td>5</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Chunk Manager</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Connection Mgr</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td></td>
<td>106</td>
<td>37</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Load Meter</td>
</tr>
<tr>
<td>8</td>
<td>6240</td>
<td></td>
<td>7376</td>
<td>845</td>
<td>0.23%</td>
<td>0.15%</td>
<td>0.55%</td>
<td>Exec</td>
</tr>
<tr>
<td>9</td>
<td>379</td>
<td></td>
<td>62</td>
<td>6112</td>
<td>0.00%</td>
<td>0.07%</td>
<td>0.04%</td>
<td>Check heaps</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Pool Manager</td>
</tr>
<tr>
<td>11</td>
<td>3</td>
<td></td>
<td>2</td>
<td>1500</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Timers</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>AAA_SERVER_DEADT</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>AAA high-capacit</td>
</tr>
<tr>
<td>14</td>
<td>307</td>
<td></td>
<td>517</td>
<td>593</td>
<td>0.00%</td>
<td>0.05%</td>
<td>0.03%</td>
<td>EnvMon</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>OIR Handler</td>
</tr>
<tr>
<td>16</td>
<td>283</td>
<td></td>
<td>58</td>
<td>4879</td>
<td>0.00%</td>
<td>0.04%</td>
<td>0.02%</td>
<td>ARP Input</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>Serial Backgroun</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td></td>
<td>81</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>ALARM_TRIGGER_SC</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>DDR Timers</td>
</tr>
</tbody>
</table>

---

**Cisco IOS Configuration Fundamentals Command Reference**

show monitor permit list through show process memory

850
The table below describes the significant fields shown in the display.

### Table 155: show processes cpu detailed (Software Modularity) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total CPU utilization for five seconds</td>
<td>Total CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.</td>
</tr>
<tr>
<td>1 minute</td>
<td>CPU utilization for the last minute.</td>
</tr>
<tr>
<td>5 minutes</td>
<td>CPU utilization for the last 5 minutes.</td>
</tr>
<tr>
<td>PID/TID</td>
<td>Process ID or task ID.</td>
</tr>
<tr>
<td>5Sec</td>
<td>Percentage of CPU time spent at the interrupt level for this process during the last five seconds.</td>
</tr>
<tr>
<td>1Min</td>
<td>Percentage of CPU time spent at the interrupt level for this process during the last minute.</td>
</tr>
<tr>
<td>5Min</td>
<td>Percentage of CPU time spent at the interrupt level for this process during the last five minutes.</td>
</tr>
<tr>
<td>Process</td>
<td>Process name.</td>
</tr>
<tr>
<td>Prio</td>
<td>Priority level of the process.</td>
</tr>
<tr>
<td>STATE</td>
<td>Current state of the process.</td>
</tr>
<tr>
<td>CPU</td>
<td>CPU utilization of the process in minutes and seconds.</td>
</tr>
<tr>
<td>type</td>
<td>Type of process; can be either IOS or POSIX.</td>
</tr>
<tr>
<td>Task</td>
<td>Task sequence number.</td>
</tr>
<tr>
<td>Runtime(us)</td>
<td>CPU time that the process has used (in microseconds).</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process has been invoked.</td>
</tr>
<tr>
<td>uSecs</td>
<td>Microseconds of CPU time for each process invocation.</td>
</tr>
<tr>
<td>5Sec</td>
<td>CPU utilization by task in the last 5 seconds.</td>
</tr>
</tbody>
</table>
Cisco Catalyst 4500e Series Switches running IOS XE software

The following is sample output from the `show processes cpu` command:

```
Switch#show proc cpu
Core 0: CPU utilization for five seconds: 1%; one minute: 7%; five minutes: 5%
Core 1: CPU utilization for five seconds: 1%; one minute: 20%; five minutes: 12%

PID  Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1  935  596  156971 0.00  0.00  0.00  0 init
2   0   79  10405  0.00  0.00  0.00  0 kthread
3  13  2450  5575  0.00  0.00  0.00  0 migration/0
4  12  808  15237 0.00  0.00  0.00  0 ksoftirqd/0
5   8  1413  6170  0.00  0.00  0.00  0 migration/1
6  14  894  16370 0.00  0.00  0.00  0 ksoftirqd/1
7  31 1422  21961 0.00  0.00  0.00  0 events/0
8  32 1269  25403 0.00  0.00  0.00  0 events/1
9   5  637  9070  0.00  0.00  0.00  0 khelper
61  80  79  102031 0.00  0.00  0.00  0 kblockd/0
62  90  183  497142 0.00  0.00  0.00  0 kblockd/1
75   0  21  1238  0.00  0.00  0.00  0 khubd
78   0  23  652  0.00  0.00  0.00  0 kseriod
83   7  26 271115  0.00  0.00  0.00  0 kmemd
```

The following is partial sample output from the `show processes cpu` command with the `detailed` keyword:

```
switch#show proc cpu detailed
Core 0: CPU utilization for five seconds: 0%; one minute: 6%; five minutes: 5%
Core 1: CPU utilization for five seconds: 2%; one minute: 17%; five minutes: 12%

PID  T C  TID  Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1  L  935  596  156971 0.00  A  0.00  0.00  0 init
2  L   0   79  10405  0.00  A  0.00  0.00  0 kthread
3  L  13  2481  5573  0.00  A  0.00  0.00  0 migration/0
4  L  12  808  15237 0.00  A  0.00  0.00  0 ksoftirqd/0
5  L  8  1454  6157  0.00  A  0.00  0.00  0 migration/1
6  L  14  897  16341 0.00  A  0.00  0.00  0 ksoftirqd/1
7  L  31 1471  21661 0.00  A  0.00  0.00  0 events/0
8  L  33 1308  25496 0.00  A  0.00  0.00  0 events/1
9  L  5  637  9070  0.00  A  0.00  0.00  0 khelper
61  L  80  79  102031 0.00  A  0.00  0.00  0 kblockd/0
62  L  90  183  497142 0.00  A  0.00  0.00  0 kblockd/1
75  L  0  21  1238  0.00  A  0.00  0.00  0 khubd
78  L  0  23  652  0.00  A  0.00  0.00  0 kseriod
83  L  7  26 271115  0.00  A  0.00  0.00  0 kmemd
```

Cisco IOS Configuration Fundamentals Command Reference
The following is sample output from the `show processes cpu history summary` command:

```
Switch#show processes cpu history summary
History information for system:

CPU% per second (last 60 seconds)
* = maximum CPU%  # = average CPU%

The following is sample output from the `show processes cpu history detailed` command:

Switch#show processes cpu history detailed
History information for core 0:
```
show processes cpu

show monitor permit list through show process memory

show processes cpu
Switch# show proc cpu history table
CPU utilization for five seconds: 1%/0% at 01:14:44
  PID  5Sec  Process
10319  6  iosd
CPU utilization for five seconds: 1%/0% at 01:14:49
  PID  5Sec  Process
10319  6  iosd
CPU utilization for five seconds: 1%/0% at 01:14:54
  PID  5Sec  Process
10319  6  iosd
CPU utilization for five seconds: 1%/0% at 01:14:59
  PID  5Sec  Process
10319  6  iosd
Switch#

The table below describes the fields shown in the output.

**Table 156: show processes cpu Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core (#)</td>
<td>Core for which CPU utilization is being generated.</td>
</tr>
<tr>
<td>CPU utilization for five seconds</td>
<td>CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.</td>
</tr>
<tr>
<td>one minutes</td>
<td>CPU utilization for the last minute.</td>
</tr>
<tr>
<td>five minutes</td>
<td>CPU utilization for the last 5 minutes.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Runtime (us)</td>
<td>CPU time that the process has used (in microseconds).</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process has been invoked.</td>
</tr>
<tr>
<td>uSecs</td>
<td>Microseconds of CPU time for each process invocation.</td>
</tr>
</tbody>
</table>
### show processes detailed

To display detailed information about POSIX and Cisco IOS processes when Cisco IOS Software Modularity or Cisco IOS XE images are running, use the `show processes detailed` command in user EXEC or privileged EXEC mode.

**Syntax**

`show processes detailed [ {process-id process-name} ]`

**Cisco Catalyst 4500e Series Switches running IOS XE software**

`show processes detailed [process-id]`

**Syntax Description**

- `process` (Optional) Shows details about a specific process.
- `process-id` (Optional) Process identifier.
- `process-name` (Optional) Process name.

**Command Default**

If no process ID or process name is specified, detailed information is displayed about all processes.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXF4</td>
<td>This command was introduced to support Software Modularity images.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1.0.SG</td>
<td>This command was introduced on the Cisco Catalyst 4500e Series</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show processes detailed` command to gather detailed information about the number of tasks running, the process state, and other information about a process that is not displayed by the `show processes` command.

---

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5Sec</td>
<td>CPU utilization by task in the last 5 seconds.</td>
</tr>
<tr>
<td>1Min</td>
<td>CPU utilization by task in the last minute.</td>
</tr>
<tr>
<td>5Min</td>
<td>CPU utilization by task in the last 5 minutes.</td>
</tr>
<tr>
<td>TTY</td>
<td>Terminal that controls the process.</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the process.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes</td>
<td>Displays information about active processes.</td>
</tr>
<tr>
<td>show processes memory</td>
<td>Displays the amount of system memory used per system process.</td>
</tr>
</tbody>
</table>
On Cisco IOS XE images, **show process detailed** will also show **process, thread and task** details.

**Examples**

Example output varies between Cisco IOS software images and Cisco Catalyst 4500e Series Switches running IOS XE software. The following sections show output examples for each image.

**Cisco IOS Software**

The following is sample output from the **show processes detailed** command for the process named `sysmgr.proc`:

```
Router# show processes detailed sysmgr.proc
   Job Id: 67
         PID: 8210
       Executable name: sysmgr.proc
       Executable path: sbin/sysmgr.proc
       Instance ID: 1
                 Args: -p
             Respawn: ON
         Respawn count: 1
       Max. spawns per minute: 30
                  Last started: Mon Aug 18 17:08:53 2003
            Process state: Run
               core: SHAREDMEM MAINMEM
          Max. core: 0
            Level: 39

         PID   TID   Stack pri state  Blked HR:MM:SS:MSEC  FLAGS  NAME
            8210  1    52K  10  Receive 1  0:00:00:0071  00000000  sysmgr.proc
            8210  2    52K  10  Sigwaitinfo 0:00:00:0000  00000000  sysmgr.proc
            8210  3    52K  10  Receive 8  0:00:00:0003  00000000  sysmgr.proc
            8210  4    52K  10  Reply 1  0:00:00:0003  00000000  sysmgr.proc
            8210  5    52K  10  Receive 1  0:00:00:0000  00000000  sysmgr.proc
            8210  6    52K  10  Receive 1  0:00:00:0015  00000000  sysmgr.proc
            8210  7    52K  10  Receive 1  0:00:00:0000  00000000  sysmgr.proc
            8210  8    52K  10  Receive 1  0:00:00:0000  00000000  sysmgr.proc

   Job Id: 78
         PID: 12308
       Executable name: sysmgr.proc
       Executable path: sbin/sysmgr.proc
       Instance ID: 2
                 Args: -p
             Respawn: ON
         Respawn count: 1
       Max. spawns per minute: 30
                  Last started: Mon Aug 18 17:08:54 2003
            Process state: Run
               core: SHAREDMEM MAINMEM
          Max. core: 0
            Level: 40

         PID   TID   Stack pri state  Blked HR:MM:SS:MSEC  FLAGS  NAME
            12308  1    16K  10  Receive 1  0:00:00:0039  00000000  sysmgr.proc
            12308  2    16K  10  Sigwaitinfo 0:00:00:0000  00000000  sysmgr.proc
```

---

857
Cisco Catalyst 4500e Series Switches running IOS XE software

The following is sample output from the `show processes detailed` command showing details of the `iosd` process:

```
Switch#show proc cpu
Switch#show processes detailed process iosd
Process Id : 10319
Process Name : iosd
Parent Process Id : 9416
Group Id : 10319
Status : Sl
Session Id : 9415
User Time : 7875
Kernel Time : 2281
Priority :
Virtual Bytes : 1819336
Resident Pages : 953636
Resident Limit : 4194303
Minor PageFaults : 238050
Major PageFaults : 1088
Cmdline arguments : -n 2048 -m 256 -l lanbase
Thread Listing:
 PID  C  TID  Stack  Pri  TTY  NAME
10319  1 10319 84  20  0  load
10319  0 10873 84  30  0  load
10319  0 10874 84  20  0  load
Task Listing:
 PID  Qty  PC  Runtime(ms)  Invoked  uSecs  Stacks  TTY  Process
1  Cwe  29764508 4  7  0  504/35000  0  Chunk Manager
2  Cap  28101409 0  85  0  408/32000  0  Load Meter
3  Hwe  26994556 0  1  0  328/35000  0  Deferred Events
4  Mwe  27835771 0  6  0  7816/35000  0  SpanTree Helper
5  Mwe  27139064 0  1  0  328/35000  0  Retransmission of I
6  Mwe  27138527 0  1  0  328/35000  0  IPC ISSU Receive Pr
7  Lst  29780794 220 45  0  424/35000  0  Check heaps
8  Cwe  29784274 0  9  0  520/35000  0  Pool Manager
9  Mst  28412237 0  2  0  456/35000  0  load
10 Mwe  27212830 0  2  0  472/35000  0  Serial Background
11 Mwe  28504055 32 22  0  3176/35000  0  RF Slave Main Threa
12 Mwe  27808556 0  1  0  344/35000  0  ifIndex Receive Pro
13 Mwe  27917322 12 91  0  552/35000  0  IOSD ipc task
14 Mwe  27917339 0  2  0  584/53000  0  IOSD chasfs task
15 Mwe  28318114 0  2  0  1384/35000  0  cpf_msg_holdq_proce
16 Mwe  27927986 4  94  0  4904/35000  0  IOSd System Config
17 Cwe  27917853 0  227 0  536/35000  0  IOSD heartbeat proc
18 Mwe  28152849 8  14  0  488/35000  0  ARP Input
19 Lwe  28315806 0  1  0  312/35000  0  CEF MIB API
20 Lwe  28397268 0  1  0  280/35000  0  AAA_SERVER_DEADTIME
21 Mwe  28394584 0  2  0  456/35000  0  AAA high-capacity c
22 Mwe  28495535 0  1  0  392/41000  0  Policy Manager
23 Lwe  28553141 0  7  0  696/35000  0  Entity MIB API
24 Mwe  28793021 0  1  0  296/35000  0  IFS Agent Manager
```

The table below describes the significant fields shown in the display.
### Table 157: show processes detailed Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Id</td>
<td>Job identifier.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Executable name</td>
<td>Process name.</td>
</tr>
<tr>
<td>Executable path</td>
<td>Path and filename of the process.</td>
</tr>
<tr>
<td>Instance ID</td>
<td>Instance number.</td>
</tr>
<tr>
<td>Args</td>
<td>Arguments sent to the process at startup.</td>
</tr>
<tr>
<td>Respawn</td>
<td>Ability to respawn process: on or off.</td>
</tr>
<tr>
<td>Respawn count</td>
<td>Number of respawns of this process since boot where boot equals one.</td>
</tr>
<tr>
<td>Max. spawns per minute</td>
<td>Maximum number of respawns per minute for this process.</td>
</tr>
<tr>
<td>Last started</td>
<td>Date and time the process was last started.</td>
</tr>
<tr>
<td>Process state</td>
<td>Current state of process.</td>
</tr>
<tr>
<td>Core</td>
<td>Core dump options specified for the process.</td>
</tr>
<tr>
<td>Max. core</td>
<td>Maximum number of dumps allowed for this process.</td>
</tr>
<tr>
<td>Level</td>
<td>Internal number that determines the startup order for the process.</td>
</tr>
<tr>
<td>TID</td>
<td>Thread ID.</td>
</tr>
<tr>
<td>Stack</td>
<td>Size, in kilobytes, of the memory stack.</td>
</tr>
<tr>
<td>pri</td>
<td>Process priority.</td>
</tr>
<tr>
<td>state</td>
<td>Current state of process.</td>
</tr>
<tr>
<td>Blked</td>
<td>Thread (with given process ID) that is currently blocked by the process.</td>
</tr>
<tr>
<td>HR:MM:SS:MSEC</td>
<td>Time (in hours, minutes, seconds, and milliseconds) used by the process.</td>
</tr>
<tr>
<td>FLAGS</td>
<td>Process flags (bitmask).</td>
</tr>
<tr>
<td>NAME</td>
<td>Process name.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes</td>
<td>Displays information about active processes.</td>
</tr>
</tbody>
</table>
show processes interrupt mask buffer

To display information in the interrupt mask buffer, use the `show processes interrupt mask buffer` command in privileged EXEC mode.

```
show processes interrupt mask buffer
```

| buffer | Displays stack trace and information about the places where interrupts have been masked more than the configured threshold time. |

**Command Modes**  
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show processes interrupt mask buffer` command. The output displays stack trace and relevant information about the places where interrupts have been masked more than the configured threshold time:

```
Router# show processes interrupt mask buffer
Allowable interrupt mask time : 50 micro seconds
Allowable number of half pipeline ticks for this platform : 5000
Buffer Size : 50 entries
NETS Disable : 3
TTY Disable : 4
ALL Disable : 4
disable_interrupts : 12
PID Level Time Spent(us) Count Stack Trace
3 11 360 1 0x608C3C14 0x60894748 0x6089437C 0x608943AC 0x609CEC88 0x609CECF0 0x609C8524
3 11 322 1 0x608C3C14 0x609CEC88 0x609CECF0 0x609C8524 0x60867C28 0x607C70B0
3 4 147 1 0x6078AED4 0x6078BE94 0x60787C50 0x6078C8D4 0x607E27F0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear processes interrupt mask detail</td>
<td>Clears the interrupt masked details for all processes and stack traces which have been dumped into the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask profile</td>
<td>Enables or disables interrupt mask profiling for all processes running on the system.</td>
</tr>
<tr>
<td>scheduler interrupt mask size</td>
<td>Configures the maximum number of entries that can exist in the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask time</td>
<td>Configures the maximum amount of time a process can run with interrupts masked.</td>
</tr>
<tr>
<td>show processes interrupt mask detail</td>
<td>Displays interrupt masked details for the specified process or all processes in the system.</td>
</tr>
</tbody>
</table>
show processes interrupt mask detail

To display information about interrupt masking, use the `show processes interrupt mask detail` command in privileged EXEC mode.

`show processes interrupt mask detail [pid]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>Displays information about the total amount of time and the number of times interrupts have been masked by all processes.</td>
</tr>
<tr>
<td><code>pid</code></td>
<td>(Optional) An integer that specifies the process id for which to display the total accumulated time and the number of times interrupts have been masked.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show processes interrupt mask detail` command. The output displays information about the total amount of time and number of times interrupts have been masked by all processes:

```
Router# show processes interrupt mask detail
PID  Time Spent(us)  Count  Process Name
 2    6388          1791  Load Meter
 3    7957          16831  Exec
 5    6710          2813  Check heaps
```

The following is sample output from the `show processes interrupt mask detail` command with the process ID specified. The output displays the total time (accumulative), number of times interrupts have been masked by a specific process:

```
Router# show processes interrupt mask detail 2
Process ID : 2
    Process Name : Load Meter
    Total Interrupt Masked Time : 6586 (us)
    Total Interrupt Masked Count : 1845
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear processes interrupt mask detail</td>
<td>Clears the interrupt masked details for all processes and stack traces which have been dumped into the interrupt mask buffer.</td>
</tr>
<tr>
<td>scheduler interrupt mask profile</td>
<td>Enables or disable interrupt mask profiling for all processes running on the system.</td>
</tr>
<tr>
<td>scheduler interrupt mask size</td>
<td>Configures the maximum number of entries that can exist in the interrupt mask buffer.</td>
</tr>
</tbody>
</table>
**show processes memory**

To display the amount of memory used by each system process in Cisco IOS, Cisco IOS XE, or Cisco IOS Software Modularity images, use the `show processes memory` command in privileged EXEC mode.

**Cisco IOS Software**

```
show processes memory [{process-id|sorted [{allocated|getbufs|holding}]]}
```

**Cisco IOS Software Modularity**

```
show processes memory [{[detailed [{process-name[:instance-id]]|process-id task-id}] | [alloc-summary|sorted {start|size|caller}]}
```

**Cisco Catalyst 4500e Series Switches Running IOS XE software**

```
show processes memory [{detailed [{process iosd|task task-id}]|sorted [{allocated|getbufs|holding}]]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Cisco IOS Software Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>process-id</strong></td>
<td>(Optional) Process ID (PID) of a specific process. When you specify a process ID, only details for the specified process will be shown.</td>
</tr>
<tr>
<td><strong>sorted</strong></td>
<td>(Optional) Displays memory data sorted by the Allocated,Getbufs,or Holding column. If the <code>sorted</code> keyword is used by itself, data is sorted by the Holding column by default.</td>
</tr>
<tr>
<td><strong>allocated</strong></td>
<td>(Optional) Displays memory data sorted by the Allocated column.</td>
</tr>
<tr>
<td><strong>getbufs</strong></td>
<td>(Optional) Displays memory data sorted by the Getbufs (Get Buffers) column.</td>
</tr>
<tr>
<td><strong>holding</strong></td>
<td>(Optional) Displays memory data sorted by the Holding column. This keyword is the default.</td>
</tr>
<tr>
<td><strong>detailed</strong></td>
<td>(Optional) Displays detailed information about iosproc processes.</td>
</tr>
<tr>
<td><strong>process-name</strong></td>
<td>(Optional) Process name.</td>
</tr>
<tr>
<td><strong>: instance-id</strong></td>
<td>(Optional) Instance name of either the Cisco IOS task or POSIX process. The colon is required.</td>
</tr>
<tr>
<td><strong>process-id</strong></td>
<td>(Optional) Process identifier.</td>
</tr>
</tbody>
</table>
Cisco IOS Software Syntax

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskid</td>
<td>(Optional) Displays detailed memory usage of a specified Cisco IOS task within a process.</td>
</tr>
<tr>
<td>alloc-summary</td>
<td>(Optional) Displays summary POSIX process memory usage per allocator.</td>
</tr>
<tr>
<td>sorted</td>
<td>(Optional) Displays POSIX process memory usage sorted by start address, size, or the PC that called the process.</td>
</tr>
<tr>
<td>start</td>
<td>(Optional) Displays POSIX process memory usage sorted by the start address of the process.</td>
</tr>
<tr>
<td>size</td>
<td>(Optional) Displays POSIX process memory usage sorted by the size of the process.</td>
</tr>
<tr>
<td>caller</td>
<td>(Optional) Displays POSIX process memory usage sorted by the PC that called the process.</td>
</tr>
</tbody>
</table>

Command Default

The memory used by all types of system processes is displayed.

Cisco IOS XE Software and Software Modularity

The system memory followed by a one-line summary of memory information about each IOS XE or Software Modularity process is displayed.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>sorted</code>, <code>allocated</code>, <code>getbufs</code>, and <code>holding</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(13)</td>
<td>The <code>sorted</code>, <code>allocated</code>, <code>getbufs</code>, and <code>holding</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(13)S</td>
<td>The <code>sorted</code>, <code>allocated</code>, <code>getbufs</code>, and <code>holding</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>sorted</code>, <code>allocated</code>, <code>getbufs</code>, and <code>holding</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(28)S</td>
<td>The output of the header line was updated to support the Memory Thresholding feature.</td>
</tr>
<tr>
<td>12.2(22)S</td>
<td>The output of the header line was updated to support the Memory Thresholding feature.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>The output of the header line was updated to support the Memory Thresholding feature.</td>
</tr>
</tbody>
</table>
The summary information (first lines of output) for this command was separated from the rest of the output and labeled by memory pool type (Total Process Memory, Total I/O Memory, and so on).

This enhancement also corrected a total process memory mismatch error (mismatch between the `show processes memory` command, the `show processes memory sorted` command, and the `show memory` command and its variants).

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(30)S</td>
<td>The summary information (first lines of output) for this command was separated from the rest of the output and labeled by memory pool type (Total Process Memory, Total I/O Memory, and so on). This enhancement also corrected a total process memory mismatch error (mismatch between the <code>show processes memory</code> command, the <code>show processes memory sorted</code> command, and the <code>show memory</code> command and its variants).</td>
</tr>
<tr>
<td>12.2(28)S</td>
<td>The summary information (first lines of output) for this command was separated from the rest of the output and labeled by memory pool type (Total Process Memory, Total I/O Memory, and so on). This enhancement also corrected a total process memory mismatch error (mismatch between the <code>show processes memory</code> command, the <code>show processes memory sorted</code> command, and the <code>show memory</code> command and its variants).</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The summary information (first lines of output) for this command was separated from the rest of the output and labeled by memory pool type (Total Process Memory, Total I/O Memory, and so on). This enhancement also corrected a total process memory mismatch error (mismatch between the <code>show processes memory</code> command, the <code>show processes memory sorted</code> command, and the <code>show memory</code> command and its variants).</td>
</tr>
<tr>
<td>12.2(18)SXF4</td>
<td>The syntax was modified to support Cisco IOS Software Modularity images.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1.0.SG</td>
<td>This command was introduced on the Cisco Catalyst 4500e Series Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show processes memory` command and the `show processes memory sorted` command display a summary of total, used, and free memory, followed by a list of processes and their memory impact.

If the standard `show processes memory process-id` command is used, processes are sorted by their PID. If the `show processes memory sorted` command is used, the default sorting is by the Holding value.

**Output Prior to Releases 12.3(7)T, 12.2(22)S, and 12.0(28)S**

The first line (header line) of the `show processes memory[sorted]` command listed Total memory, Used memory, and Free memory values.

**Output in Releases 12.3(7)T, 12.3(8)T, and 12.2(22)S Through 12.2(27)S2, 12.0(28)S, and 12.0(29)S**

In Releases 12.3(7)T, 12.2(22)S, and 12.0(28)S, the Memory Thresholding feature was introduced. This feature affected the header line and the Holding column of the `show processes memory` command as described in this section.

The value for Total in the `show processes memory` command and the values listed in the Holding column showed the total (cumulative) value for the processor memory pools and the alternate memory pool* (typically, the I/O memory pool). However, the `show processes memory sorted` version of this command, and other
commands, such as the `show memory summary` command, did not include the alternate memory pool in the totals; that is, these commands showed the total value for the Processor memory pool only. This caused an observed mismatch of memory totals between commands.

If you are using these releases, use the output of the `show memory summary` command to determine the individual amounts of Total and Free memory for the Processor memory pool and the I/O memory pool.

**Output in Releases 12.3(11)T, 12.2(28)S, 12.0(30)S, and Later Releases**

Beginning in Releases 12.3(11)T, 12.2(28)S, and 12.0(30)S, the summary information (first output lines) for the `show processes memory` command is separated by memory pool. For example, there are now individual lines for Total Process Memory, Total I/O Memory, and Total PCI Memory. In these releases or later releases, your Total Process Memory should match the total process memory shown for other commands, such as the `show memory summary` command.

**About Alternate Memory Pools**

An “alternate memory pool” is a memory pool that can be used as an alternative to allocate memory when the target (main) memory pool has been filled. For example, many platforms have a memory type called “Fast” that is limited to a small size (because the memory media used for Fast memory is expensive). You can prevent memory allocations from failing once the available Fast memory has been used up, by configuring the normal Processor memory as an alternative memory pool for the Fast memory pool.

**Cisco IOS XE Software and Software Modularity**

Use the `show processes memory` command without any arguments and keywords to display the system memory followed by a one-line summary of memory information about each modular Cisco IOS process. Use the `detailed` keyword with this command to display detailed memory information about all processes. Other arguments and keywords are used to display Cisco IOS Software Modularity process memory information for a specified process name or process ID.

On Cisco IOS XE images only, the `detailed` keyword will also show Cisco IOS task memory details.

**show processes memory Command for Cisco IOS Releases Prior to 12.3(7)T, 12.2(22)S, and 12.0(28)S**

The following is sample output from the `show processes memory` command:

```bash
Router# show processes memory
Processor Pool Total: 25954228 Used: 8368640 Free: 17585588
PID TTY Allocated Freed Holding Getbufs Retbufs Process
0 0 8629528 6990 6751716 0 0 *Init*
0 0 24048 12928 24048 0 0 *Sched*
0 0 260 328 68 350080 0 *Dead*
1 0 0 0 12928 0 0 Chunk Manager
2 0 192 192 6928 0 0 Load Meter
3 0 214664 304 227288 0 0 Exec
4 0 0 0 12928 0 0 Check heaps
5 0 0 0 12928 0 0 Pool Manager
6 0 192 192 12928 0 0 Timers
7 0 192 192 12928 0 0 Serial Background
8 0 192 192 12928 0 0 AAA high-capacity
9 0 0 0 24928 0 0 Policy Manager
10 0 0 0 12928 0 0 ARP Input
11 0 192 192 12928 0 0 DDR Timers
12 0 0 0 12928 0 0 Entity MIB API
13 0 0 0 12928 0 0 MPLS HC Counter
14 0 0 0 12928 0 0 SERIAL A’detect
```
The table below describes the significant fields shown in the display.

Table 158: show processes memory Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Pool Total</td>
<td>Total amount of memory, in kilobytes (KB), held for the Processor memory pool.</td>
</tr>
<tr>
<td>Used</td>
<td>Total amount of used memory, in KB, in the Processor memory pool.</td>
</tr>
<tr>
<td>Free</td>
<td>Total amount of free memory, in KB, in the Processor memory pool.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>TTY</td>
<td>Terminal that controls the process.</td>
</tr>
<tr>
<td>Allocated</td>
<td>Bytes of memory allocated by the process.</td>
</tr>
<tr>
<td>Freed</td>
<td>Bytes of memory freed by the process, regardless of who originally allocated it.</td>
</tr>
<tr>
<td>Holding</td>
<td>Amount of memory, in KB, currently allocated to the process.</td>
</tr>
<tr>
<td>Getbufs</td>
<td>Number of times the process has requested a packet buffer.</td>
</tr>
<tr>
<td>Retbufs</td>
<td>Number of times the process has relinquished a packet buffer.</td>
</tr>
<tr>
<td>Process</td>
<td>Process name.</td>
</tr>
<tr>
<td><em>Init</em></td>
<td>System initialization process.</td>
</tr>
<tr>
<td><em>Sched</em></td>
<td>The scheduler process.</td>
</tr>
<tr>
<td><em>Dead</em></td>
<td>Processes as a group that are now dead.</td>
</tr>
<tr>
<td>&lt;value&gt; Total</td>
<td>Total amount of memory, in KB, held by all processes (sum of the “Holding” column).</td>
</tr>
</tbody>
</table>

The following is sample output from the `show processes memory` command when the `sorted` keyword is used. In this case, the output is sorted by the Holding column, from largest to smallest.

```
Router# show processes memory sorted
Processor Pool Total: 25954228  Used: 8371280  Free: 17582948
PID  TTY  Allocated  Freed  Holding  Getbufs  Retbufs  Process
 0    0     8629528   689900   6751716      0      0   *Init*
 3    0     217304    304     229928      0      0     Exec
53   0     109248    192     96064      0      0   DHCPD Receive
56   0      12192     0     32928      0      0      COPS
19   0     176704    192     25192      0      0   Net Background
42   0      19872     0     24960      0      0     L2X Data Daemon
58   0      192      0     24928      0      0     X.25 Background
43   0      192      0     24928      0      0     FPF IP Route
49   0      192      0     24928      0      0     TCP Protocols
48   0      192      0     24928      0      0     TCP Timer
17   0      192      0     24928      0      0     XML Proxy Client
```
The following is sample output from the `show processes memory` command when a process ID (process-id) is specified:

```
Router# show processes memory 1

Process ID: 1
Process Name: Chunk Manager
Total Memory Held: 8428 bytes
Processor memory holding = 8428 bytes
  pc = 0x60790654, size = 6044, count = 1
  pc = 0x6076DBC4, size = 652, count = 1
  pc = 0x6076FF18, size = 188, count = 1
I/O memory holding = 0 bytes
```

```
Router# show processes memory 2

Process ID: 2
Process Name: Load Meter
Total Memory Held: 3884 bytes
Processor memory holding = 3884 bytes
  pc = 0x60790654, size = 3044, count = 1
  pc = 0x6076DBC4, size = 652, count = 1
  pc = 0x6076FF18, size = 188, count = 1
I/O memory holding = 0 bytes
```

**show processes memory Command for Cisco IOS Releases Prior to 12.3(11)T, 12.2(28)S, and 12.0(30)S**

The following example shows the output of the `show processes memory` command before the changes to the summary information were made. Note that the Total in the `show processes summary` command output indicates total memory for all memory pools; in this example, the `show processes memory` total of 35423840 can be obtained by adding the Processor and I/O totals shown in the output of the `show memory summary` command. Note also that the `show processes memory sorted` command lists the Total Processor Memory (matches the `show memory summary` Processor Total), but the `show processes memory` command (without the `sorted` keyword) lists the total for all memory pools (Processor plus I/O memory).

```
Router# show version | include IOS
Cisco IOS Software, 3600 Software (C3660-BIN-M), Version 12.3(9)
Router# show memory summary
  Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 61E379A0 27035232 8089056 18946176 17964108 17963664
  I/O 38000000 8388608 2815088 5573520 5561520 5573472
```

```
Router# show processes memory
```
### show processes memory

```
Total: 35423840
, Used: 10904192, Free: 24519648

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>Allocated</th>
<th>Freed</th>
<th>Holding</th>
<th>Getbufs</th>
<th>Retbufs</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>14548868</td>
<td>3004980</td>
<td>9946092</td>
<td>0</td>
<td>0</td>
<td><em>Init</em></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>12732</td>
<td>567448</td>
<td>12732</td>
<td>0</td>
<td>0</td>
<td><em>Sched</em></td>
</tr>
</tbody>
</table>

Router# show processes memory sorted

Total: 27035232
, Used: 8089188, Free: 18946044

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>Allocated</th>
<th>Freed</th>
<th>Holding</th>
<th>Getbufs</th>
<th>Retbufs</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>14548868</td>
<td>3004980</td>
<td>9946092</td>
<td>0</td>
<td>0</td>
<td><em>Init</em></td>
</tr>
<tr>
<td>64</td>
<td>0</td>
<td>76436</td>
<td>3084</td>
<td>74768</td>
<td>0</td>
<td>0</td>
<td>CEF process</td>
</tr>
</tbody>
</table>

Router# show version | include IOS

Cisco IOS Software, 3600 Software (c3660-p-mz), Version 12.0(29)S,

Router# show memory summary

<table>
<thead>
<tr>
<th>Head</th>
<th>Total(b)</th>
<th>Used(b)</th>
<th>Free(b)</th>
<th>Lowest(b)</th>
<th>Largest(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>126CB10</td>
<td>49,331,668</td>
<td>6454676</td>
<td>42876992</td>
<td>42642208</td>
</tr>
</tbody>
</table>

Router# show processes memory

Total: 50,994,868
, Used: 6222644, Free: 44772224

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>Allocated</th>
<th>Freed</th>
<th>Holding</th>
<th>Getbufs</th>
<th>Retbufs</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>6796228</td>
<td>627336</td>
<td>5325956</td>
<td>0</td>
<td>0</td>
<td><em>Init</em></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>200</td>
<td>29792</td>
<td>200</td>
<td>0</td>
<td>0</td>
<td><em>Sched</em></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>192</td>
<td>744</td>
<td>0</td>
<td>349000</td>
<td>0</td>
<td><em>Dead</em></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12896</td>
<td>0</td>
<td>0</td>
<td>Chunk Manager</td>
</tr>
</tbody>
</table>

Router# show processes memory sorted

Total: 50,994,868
, Used: 6222644, Free: 44772224

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>Allocated</th>
<th>Freed</th>
<th>Holding</th>
<th>Getbufs</th>
<th>Retbufs</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>6796228</td>
<td>627336</td>
<td>5325956</td>
<td>0</td>
<td>0</td>
<td><em>Init</em></td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>39056</td>
<td>0</td>
<td>25264</td>
<td>0</td>
<td>0</td>
<td>Net Background</td>
</tr>
<tr>
<td>48</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>24896</td>
<td>0</td>
<td>0</td>
<td>L2X SSS manager</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>24896</td>
<td>0</td>
<td>0</td>
<td>IP Input</td>
</tr>
</tbody>
</table>

### show processes memory Command for Cisco IOS Software Modularity

In a Cisco IOS Software Modularity image IOS, each process maintains its own heap memory, which is taken from the system memory in blocks. The process reuses this memory as required. If all the memory that was requested in a block is no longer in use, then the process can return the memory block to the system.

The following is sample output from the `show processes memory` command when a Cisco IOS Software Modularity image is running:

```
Router# show processes memory
System Memory : 262144K total, 113672K used, 148472K free
```
The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>Total amount of memory, in KB, on the device.</td>
</tr>
<tr>
<td>used</td>
<td>Amount of memory, in KB, used in the system.</td>
</tr>
<tr>
<td>free</td>
<td>Amount of free memory, in KB, available in the system.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>Text</td>
<td>Amount of memory, in KB, used by the text segment of the specified process.</td>
</tr>
<tr>
<td>Data</td>
<td>Amount of memory, in KB, used by the data segment of the specified process.</td>
</tr>
<tr>
<td>Stack</td>
<td>Amount of memory, in KB, used by the stack segment of the specified process.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>Amount of memory, in KB, used by the dynamic segment of the specified process.</td>
</tr>
<tr>
<td>Total</td>
<td>Total amount of memory, in KB, used by the specified process.</td>
</tr>
<tr>
<td>Process</td>
<td>Process name.</td>
</tr>
</tbody>
</table>
The following example shows the output of the `show processes memory detailed` command wherein the process (ios-base) holds sufficient memory to process a request of the Cisco IOS tasks without having to request more memory from the system. So although the amount of memory of the Cisco IOS tasks increased, the ios-base process does not consume more system memory.

Router# show processes memory detailed 16424 sorted holding
System Memory : 2097152K total, 1097777K used, 999375K free, 0K kernel reserved
Lowest(b) : 1017212928
Process sbin/ios-base, type IOS, PID = 16424
  248904K total, 0K text, 0K data, 168K stack, 248736K dynamic
  Heap : 385874960 total, 261213896 used, 124661064 free
Task  TTY Allocated  Freed  Holding  Getbufs  Retbufs TaskName
  0   0  156853816  11168  156365472   0   0  *Init*
  38   0  65671128  3320184  62248368   0   0  PF_Init Process
  661   0  73106800  38231816  33093704   0   0  PIM Process
  487   0  2656186248 3806507384 33039576   0   0   cmfib
  652   0  56256064  19166160  27087872   0   0  MFIB_mrib_read
  4   0  91088216  68828800  13093720   0   0  Service Task
  629   0  2059320  132840  19273920   0   0  Const2 IPv6 Pro
  49   0  2155730560 2153990528 1741536  0  9579588  DiagCard1/-1
  0   0  2510481432 1396998880 1463056  2804860  23260  *Dead*
  444   0  7333952  5940064  1410992   0   0   FM core
  411   0 12865536  7934952  1396544   0   0  CMET MGR
  310   0 113849160 121164584 1284240   0   0   Exec

The following is sample output from the `show processes memory` command with details about the memory of process 12322 and the task with the ID of 1:

Router# show processes memory detailed 12322 taskid 1
System Memory : 262144K total, 113456K used, 148688K free
Process sbin/c7200-p-blob, type IOS, PID = 12322
  16568K total, 16K text, 8K data, 64K stack, 16480K dynamic
Memory Summary for TaskID = 1
Holding = 10248
  PC  Size  Count
  0x7322FC74  9192   1
  0x73236538  640   1
  0x73231E8C  256   1
  0x74175060  160   1

The table below describes the significant fields shown in the display that are different from the table above.

**Table 160: show processes memory detailed process-id taskid Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Type of process: POSIX or IOS.</td>
</tr>
<tr>
<td>Memory Summary for TaskID</td>
<td>Task ID.</td>
</tr>
<tr>
<td>Holding</td>
<td>Amount of memory, in bytes, currently held by the task.</td>
</tr>
<tr>
<td>PC</td>
<td>Caller PC of the task.</td>
</tr>
<tr>
<td>Size</td>
<td>Amount of memory, in bytes, used by this task.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of times that task has been called.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show processes memory` command with details about the memory of POSIX process ID 234567 with summary process memory usage per allocator:

Router# show processes memory detailed 234567 alloc-summary
System Memory : 262144K total, 113672K used, 148472K free
Process sbin/sysmgr.proc, type POSIX, PID = 12308
  404K total, 100K text, 144K data, 16K stack, 144K dynamic
  81920 heapsize, 68620 allocated, 8896 free

Allocated Blocks
<table>
<thead>
<tr>
<th>Address</th>
<th>Usize</th>
<th>Size</th>
<th>Caller</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0806C358</td>
<td>0x00000478</td>
<td>0x000004D0</td>
<td>0x721C7290</td>
</tr>
<tr>
<td>0x0806D1E0</td>
<td>0x00000128</td>
<td>0x00000130</td>
<td>0x72B90248</td>
</tr>
<tr>
<td>0x0806D318</td>
<td>0x000003678</td>
<td>0x0000036E0</td>
<td>0x72B9820C</td>
</tr>
<tr>
<td>0x0806D700</td>
<td>0x000002A0</td>
<td>0x0000022C0</td>
<td>0x72B8EB58</td>
</tr>
<tr>
<td>0x0806D770</td>
<td>0x00000058</td>
<td>0x000000660</td>
<td>0x72BA5488</td>
</tr>
<tr>
<td>0x0806D7D8</td>
<td>0x000000A0</td>
<td>0x000000B0</td>
<td>0x72BBd228</td>
</tr>
<tr>
<td>0x0806D8A8</td>
<td>0x00000200</td>
<td>0x0000020A8</td>
<td>0x721A728C</td>
</tr>
<tr>
<td>0x0806FF78</td>
<td>0x00000068</td>
<td>0x00000070</td>
<td>0x72BAA78C</td>
</tr>
<tr>
<td>0x08071438</td>
<td>0x0000005C</td>
<td>0x00000068</td>
<td>0x72B907A8</td>
</tr>
<tr>
<td>0x08071508</td>
<td>0x0000010E</td>
<td>0x00000120</td>
<td>0x72BA7AFC</td>
</tr>
<tr>
<td>0x08072840</td>
<td>0x000000A8</td>
<td>0x000000C0</td>
<td>0x7270A060</td>
</tr>
<tr>
<td>0x08072910</td>
<td>0x00000118</td>
<td>0x07273A989</td>
<td>0x72749074</td>
</tr>
<tr>
<td>0x08072A30</td>
<td>0x000000E4</td>
<td>0x000000F0</td>
<td>0x7276E987C</td>
</tr>
<tr>
<td>0x08072B28</td>
<td>0x000000B0</td>
<td>0x000000B8</td>
<td>0x7276E987C</td>
</tr>
<tr>
<td>0x08072B88</td>
<td>0x0000006C</td>
<td>0x00000078</td>
<td>0x727367A4</td>
</tr>
<tr>
<td>0x08072C68</td>
<td>0x000000B8</td>
<td>0x000000C0</td>
<td>0x7271E2A4</td>
</tr>
<tr>
<td>0x08072D30</td>
<td>0x000000D0</td>
<td>0x000000D8</td>
<td>0x7273834C</td>
</tr>
<tr>
<td>0x08072E10</td>
<td>0x00000250</td>
<td>0x00000258</td>
<td>0x7271B7A7</td>
</tr>
<tr>
<td>0x08073070</td>
<td>0x000002F4</td>
<td>0x00000300</td>
<td>0x72726484</td>
</tr>
<tr>
<td>0x08073378</td>
<td>0x000006A8</td>
<td>0x000006B0</td>
<td>0x73E4A4C4</td>
</tr>
<tr>
<td>0x08073A30</td>
<td>0x00000060</td>
<td>0x00000068</td>
<td>0x7352A9F8</td>
</tr>
<tr>
<td>0x08073B38</td>
<td>0x00000068</td>
<td>0x00000070</td>
<td>0x72B92008</td>
</tr>
<tr>
<td>0x08073BB0</td>
<td>0x00000058</td>
<td>0x000000660</td>
<td>0x72B9201C</td>
</tr>
<tr>
<td>0x08073EB8</td>
<td>0x0000002A8</td>
<td>0x0000002C0</td>
<td>0x72026FEC</td>
</tr>
<tr>
<td>0x08074028</td>
<td>0x000000A0</td>
<td>0x000000A8</td>
<td>0x721DED94</td>
</tr>
<tr>
<td>0x08078028</td>
<td>0x0000022B8</td>
<td>0x0000022C0</td>
<td>0x727446B8</td>
</tr>
<tr>
<td>0x0807CO28</td>
<td>0x00002320</td>
<td>0x00002328</td>
<td>0x72B907C4</td>
</tr>
</tbody>
</table>

Free Blocks
<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0806FFF0</td>
<td>0x00000010</td>
</tr>
<tr>
<td>0x080714A8</td>
<td>0x00000058</td>
</tr>
<tr>
<td>0x08073E18</td>
<td>0x00000098</td>
</tr>
<tr>
<td>0x08073EB8</td>
<td>0x00000018</td>
</tr>
<tr>
<td>0x08076FA0</td>
<td>0x00000028</td>
</tr>
<tr>
<td>0x080774B0</td>
<td>0x00000050</td>
</tr>
<tr>
<td>0x0807FFB8</td>
<td>0x00000048</td>
</tr>
<tr>
<td>0x08080028</td>
<td>0x000003FD8</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heapsize</td>
<td>Size of the process heap, in KB.</td>
</tr>
<tr>
<td>allocated</td>
<td>Amount of memory, in KB., allocated from the heap.</td>
</tr>
<tr>
<td>free</td>
<td>Amount of free memory, in KB., in the heap for the specified process.</td>
</tr>
</tbody>
</table>
Cisco Catalyst 4500e Series Switches Running Cisco IOS XE software

The following is sample output from the `show processes memory` command:

Switch#show proc memory

<table>
<thead>
<tr>
<th>PID</th>
<th>Text</th>
<th>Data</th>
<th>Stack</th>
<th>Dynamic</th>
<th>RSS</th>
<th>Total</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>252</td>
<td>480</td>
<td>84</td>
<td>444</td>
<td>1648</td>
<td>3648</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kthreadd</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>migration/0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>migration/1</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ksoftirqd/1</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>events/0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>events/1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>khelper</td>
</tr>
<tr>
<td>61</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kbld/0</td>
</tr>
<tr>
<td>62</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kbld/1</td>
</tr>
<tr>
<td>75</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>khubd</td>
</tr>
<tr>
<td>78</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kseriod</td>
</tr>
<tr>
<td>83</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kmcd</td>
</tr>
<tr>
<td>120</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pdflush</td>
</tr>
<tr>
<td>121</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pdflush</td>
</tr>
<tr>
<td>122</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kswapd0</td>
</tr>
<tr>
<td>123</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>aio/0</td>
</tr>
<tr>
<td>124</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>aio/1</td>
</tr>
<tr>
<td>291</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kpsmoused</td>
</tr>
<tr>
<td>309</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>rpclio/0</td>
</tr>
<tr>
<td>310</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>rpclio/1</td>
</tr>
<tr>
<td>354</td>
<td>92</td>
<td>180</td>
<td>84</td>
<td>136</td>
<td>456</td>
<td>2188</td>
<td>udevd</td>
</tr>
<tr>
<td>700</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>loop1</td>
</tr>
<tr>
<td>716</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>loop2</td>
</tr>
<tr>
<td>732</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>loop3</td>
</tr>
<tr>
<td>2203</td>
<td>424</td>
<td>164</td>
<td>84</td>
<td>132</td>
<td>1172</td>
<td>3180</td>
<td>dbus-daemon</td>
</tr>
<tr>
<td>2539</td>
<td>76</td>
<td>160</td>
<td>84</td>
<td>132</td>
<td>532</td>
<td>1788</td>
<td>portmap</td>
</tr>
<tr>
<td>2545</td>
<td>76</td>
<td>160</td>
<td>84</td>
<td>132</td>
<td>532</td>
<td>1788</td>
<td>portmap</td>
</tr>
<tr>
<td>2588</td>
<td>232</td>
<td>396</td>
<td>84</td>
<td>132</td>
<td>992</td>
<td>4596</td>
<td>sshd</td>
</tr>
<tr>
<td>2602</td>
<td>196</td>
<td>320</td>
<td>84</td>
<td>132</td>
<td>752</td>
<td>2964</td>
<td>xinetd</td>
</tr>
<tr>
<td>2606</td>
<td>196</td>
<td>320</td>
<td>84</td>
<td>132</td>
<td>748</td>
<td>2964</td>
<td>xinetd</td>
</tr>
<tr>
<td>3757</td>
<td>76</td>
<td>160</td>
<td>84</td>
<td>132</td>
<td>532</td>
<td>1788</td>
<td>vsi work/0</td>
</tr>
<tr>
<td>3758</td>
<td>76</td>
<td>160</td>
<td>84</td>
<td>132</td>
<td>532</td>
<td>1788</td>
<td>vsi work/1</td>
</tr>
</tbody>
</table>

--More--

The following is sample output from the `show processes memory detailed` command:

Switch#show proc memory detailed
The following is sample output from the `show processes memory detailed` command specifying the `iosd` process:

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>Allocated</th>
<th>Freed</th>
<th>Holding</th>
<th>Getbufs</th>
<th>Retbufs</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>2568488</td>
<td>1960496</td>
<td>676992</td>
<td>5368513</td>
<td>362940</td>
<td><em>Dead</em></td>
</tr>
</tbody>
</table>

The following is sample output from the `show processes memory sorted` command:

<table>
<thead>
<tr>
<th>PID</th>
<th>Text</th>
<th>Data</th>
<th>Stack</th>
<th>Dynamic</th>
<th>RSS</th>
<th>Total</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>10319</td>
<td>67716</td>
<td>798420</td>
<td>84</td>
<td>252</td>
<td>954524</td>
<td>1012856</td>
<td>ioad</td>
</tr>
<tr>
<td>4888</td>
<td>1132</td>
<td>200108</td>
<td>84</td>
<td>4076</td>
<td>26772</td>
<td>275408</td>
<td>ffm</td>
</tr>
</tbody>
</table>
The table below describes the significant fields shown in the display.

**Table 162: show processes memory Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Pool Total</td>
<td>Total amount of memory, in KB, held for the Processor memory pool.</td>
</tr>
<tr>
<td>I/O Pool Total</td>
<td>Total amount of memory, in KB, held for the I/O memory pool.</td>
</tr>
<tr>
<td>Used</td>
<td>Total amount of used memory, in KB, in the Processor/I/O memory pool.</td>
</tr>
<tr>
<td>Free</td>
<td>Total amount of free memory, in KB, in the Processor/I/O memory pool.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>TTY</td>
<td>Terminal that controls the process.</td>
</tr>
<tr>
<td>Allocated</td>
<td>Bytes of memory allocated by the process.</td>
</tr>
<tr>
<td>Freed</td>
<td>Bytes of memory freed by the process, regardless of who originally allocated it.</td>
</tr>
<tr>
<td>Holding</td>
<td>Amount of memory, in KB, currently allocated to the process.</td>
</tr>
<tr>
<td>Getbufs</td>
<td>Number of times the process has requested a packet buffer.</td>
</tr>
<tr>
<td>Retbufs</td>
<td>Number of times the process has relinquished a packet buffer.</td>
</tr>
<tr>
<td>Process</td>
<td>Process name.</td>
</tr>
<tr>
<td><em>Init</em></td>
<td>System initialization process.</td>
</tr>
<tr>
<td><em>Sched</em></td>
<td>The scheduler process.</td>
</tr>
<tr>
<td><em>Dead</em></td>
<td>Processes as a group that are now dead.</td>
</tr>
<tr>
<td>&lt;value&gt; Total</td>
<td>Total amount of memory, in KB, held by all processes (sum of the “Holding” column).</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show memory</code></td>
<td>Displays statistics about memory, including memory-free pool statistics.</td>
</tr>
<tr>
<td><code>show processes</code></td>
<td>Displays information about the active processes.</td>
</tr>
</tbody>
</table>
show processes memory
show protocols through showmon

• show protocols through showmon, on page 878
show protocols through showmon

show protocols

To display the configured protocols, use the **show protocols** command in user EXEC or privileged EXEC mode.

**show protocols [interface-name interface-number]**
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface-name</strong></td>
<td></td>
</tr>
</tbody>
</table>

- **voaBypassIn** --VOA-Bypass-In interface
- **voaBypassOut** --VOA-Bypass-Out interface
- **voaFilterIn** --VOA-Filter-In interface
- **voaFilterOut** --VOA-Filter-Out interface
- **voaIn** --VOA-In interface
- **voaOut** --VOA-Out interface

| interface-number | (Optional) Interface number. |
(Optional) The type of interfaces. It can be one of the following values:

- **ATM** -- ATM interface
- **Async** -- Async interface
- **Auto-Template** -- Auto-Template interface
- **BVI** -- Bridge-Group Virtual Interface
- **CDMA-Ix** -- CDMA Ix interface
- **Container** -- Container interface
- **CTunnel** -- CTunnel interface
- **Dialer** -- Dialer interface
- **Ethernet** -- Institute of Electrical Engineers (IEEE) 802.3
- **FastEthernet** -- FastEthernet IEEE 802.3
- **EsconPhy** -- ESCON interface
- **fcpa** -- Fiber Channel
- **Filter** -- Filter interface
- **multiservice** -- Multiservice interface
- **Pos-channel** -- POS Channel interfaces
- **SBC** -- Session Border Controller
- **SYSCLOCK** -- Telecom-Bus Clock Controller
- **Tunnel** -- Tunnel interface
- **Vif** -- PGM Multicast Host interface
- **Virtual-Access** -- Virtual access interface
- **Virtual-PPP** -- Virtual PPP interface
- **Virtual-Template** -- Virtual template interface
- **Virtual-TokenRing** -- Virtual interface
TokenRing

- `Vlan` -- Catalyst VLANs
- `vmi` -- Virtual Multipoint Interface

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(3)T</td>
<td>The command was integrated in a release earlier than Cisco IOS Release 12.0(3)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show protocols` command shows the global and interface-specific status of any configured Level 3 protocol.

**Examples**

The following is sample output from the `show protocols` command. The field names are self-explanatory.

```
Router# show protocols
Global values:
    Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
    Internet address is 10.4.9.14/24
vmi1 is down, line protocol is down
FastEthernet0/1 is up, line protocol is up
    Internet address is 10.4.8.14/24
ATM2/0 is administratively down, line protocol is down
ATM2/0.1 is administratively down, line protocol is down
ATM2/0.2 is administratively down, line protocol is down
ATM2/0.200 is administratively down, line protocol is down
Ethernet3/0 is administratively down, line protocol is down
Ethernet3/0.1 is administratively down, line protocol is down
Ethernet3/2 is administratively down, line protocol is down
Ethernet3/3 is administratively down, line protocol is down
ATM6/0 is administratively down, line protocol is down
SSLVPN-VIF0 is up, line protocol is up
    Interface is unnumbered. Using address of SSLVPN-VIF0 (0.0.0.0)
Virtual-Access1 is down, line protocol is down
Virtual-Template1 is down, line protocol is down
Virtual-Access2 is up, line protocol is up
Port-channel15 is down, line protocol is down
Port-channel15.1 is down, line protocol is down
Port-channel15 is down, line protocol is down
Port-channel100 is down, line protocol is down
    Interface is unnumbered. Using address of vmi1 (0.0.0.0)
Dialer3 is up, line protocol is up
```
show region

To display valid memory regions (memory mapping) in use on your system, use the `show region` command in privileged EXEC mode.

`show region [address hex-address]`

**Syntax Description**

- **address hex-address** (Optional) If a hexadecimal address is specified, this command will search the region list for the specified address.

**Command Default**
All memory regions are displayed.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(23)S.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was modified. The command output was updated to display information about free regions.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The output was updated to display heap region memory size in chunks of 16 MB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can be useful for troubleshooting system bus errors. The system encounters a bus error when the processor tries to access a memory location that either does not exist (a software error) or does not respond properly (a hardware problem).

To use the `show region` command to troubleshoot a bus error, note the memory location address from the `show version` command, the `show context` command, or from the system error message that alerted you to the bus error. The `show region` command can then be used to determine if that address is a valid memory location.

For example, in the output of the `show version` command after a system restart caused by a bus error, you will see output similar to “System restarted by bus error at PC 0x30EE546, address 0xBB4C4.” In this case, the memory location that the router tried to access is 0xBB4C4. If the address falls within one of the ranges in the `show region` output, it means that the router was accessing a valid memory address, but the hardware corresponding to that address is not responding properly. This indicates a hardware problem.

If the address reported by the bus error does not fall within the ranges displayed in the `show region` output, this error means that the router was trying to access an address that is not valid, which indicates that it is a Cisco IOS software problem.
More detailed information is available on Cisco.com in Tech Note #7949, "Troubleshooting Bus Error Crashes".

**Transient Memory Allocation**

The Transient Memory Allocation feature is enabled on platforms like the Cisco 7200 series router and the Cisco 10000 series router. This feature allocates all transient memory in a separate memory address space (separate region), so that there is no interleaving of static and transient memory blocks. Hence, the output of the `show region` command will have heap region memory size in chunks of 16 MB.

**Examples**

The following is sample output from the `show region` command:

```
Router# show region
Region Manager:
Start    End    Size(b)  Class  Media   Name
0x0C000000 0x0FFFFFFF 67108864  Iomem  R/W  iomem
0x20000000 0x2FFFFFFF 268435456 Local  R/W  extended_2
0x50000000 0x5FFFFFFF 268435456 Local  R/W  extended_1
0x60000000 0x7BFFFFFF 469762048 Local  R/W  main
0x600090F8 0x6200A07F 33560336  IText  R/O  main:text
0x62014C50 0x62F5B1EF 16016800  IData  R/W  main:data
0x62F5B1F0 0x6333500F 4038176  IBss  R/W  main:bss
0x63335010 0x6359A0D3 2511044  Local  R/W  main:saved-data
0x6359A0D4 0x6459A0D3 16777216  Local  R/W  main:heap
0x7B000000 0x7BFFFFFF 16777216  Local  R/W  main:heap
0x80000000 0x8BFFFFFF 201326592 Local  R/W  main:(main_k0)
0xA0000000 0xBFFFFFFF 201326592 Local  R/W  main:(main_k1)
Free Region Manager:
Start    End    Size(b)  Class  Media   Name
0x6459A12C 0x7AFFFFA7 380001916 Local  R/W  heap
```

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

**Table 163: show region Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Start address of the memory block.</td>
</tr>
<tr>
<td>End</td>
<td>End address of the memory block.</td>
</tr>
<tr>
<td>Size(b)</td>
<td>Size of the memory block.</td>
</tr>
<tr>
<td>Class</td>
<td>Class of the memory.</td>
</tr>
<tr>
<td>Media</td>
<td>Type of the region media. Read-only (R/O), read-write (R/W), and so on.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the region.</td>
</tr>
<tr>
<td>Iomem</td>
<td>Input/output (I/O) memory. It is a type of packet memory.</td>
</tr>
<tr>
<td>Local</td>
<td>Local memory.</td>
</tr>
<tr>
<td>IText</td>
<td>Image text memory.</td>
</tr>
<tr>
<td>IData</td>
<td>Image data memory.</td>
</tr>
<tr>
<td>IBss</td>
<td>Image blind source separation (BSS) memory.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R/W</td>
<td>Read and write memory.</td>
</tr>
<tr>
<td>R/O</td>
<td>Read-only memory.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show context</td>
<td>Displays information stored in NVRAM when an unexpected system reload (system exception) occurs.</td>
</tr>
<tr>
<td>show memory</td>
<td>Displays detailed memory statistics for the system.</td>
</tr>
<tr>
<td>show version</td>
<td>Shows hardware and software information for the system.</td>
</tr>
</tbody>
</table>

### show registry

To display the function registry information when Cisco IOS or Cisco IOS Software Modularity images are running, use the `show registry` command in user EXEC or privileged EXEC mode.

**Cisco IOS Software**

```
show registry [registry-name [registry-number]] [{brief|statistics}]
```

**Cisco IOS Software Modularity**

```
show registry [name [registry-name [registry-number]]] [{brief] name [registry-name [registry-number]]] [preemptions|rpcp status|statistics [brief] [name [registry-name [registry-number]]] [remote]] [process {process-name|process-id}]
```

#### Syntax Description

**Cisco IOS Software Syntax**

- `registry-name`  (Optional) Name of the registry to display.
- `registry-number`  (Optional) Number of the registry to display.
- `brief`  (Optional) Displays limited functions and services information.
- `statistics`  (Optional) Displays function registry statistics.

**Cisco IOS Software Modularity Syntax**

- `name`  (Optional) Displays information about a specific registry.
- `registry-name`  (Optional) Name of the registry to examine.
- `registry-number`  (Optional) Number of the registry to examine.
- `brief`  (Optional) Displays limited functions and services information.
- `preemptions`  (Optional) Displays registry preemptions information.
- `rpcp status`  (Optional) Displays status of remote procedure call (RPC) proxy.
Cisco IOS Software Syntax

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>statistics</td>
<td>(Optional) Displays function registry statistics.</td>
</tr>
<tr>
<td>remote</td>
<td>(Optional) Displays name server interactions and call statistics.</td>
</tr>
<tr>
<td>process</td>
<td>(Optional) Displays process-specific information.</td>
</tr>
<tr>
<td>process-name</td>
<td>(Optional) Process name.</td>
</tr>
<tr>
<td>process-id</td>
<td>(Optional) Process ID. Number in range from 1 to 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**
If no options are specified, registry information is displayed for all registries.

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXF4</td>
<td>Keywords and arguments were added to support Software Modularity images and this command was integrated into Cisco IOS Release 12.2(18)SXF4.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**
Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. To view the appropriate output, choose one of the following sections:

- Cisco IOS Software
- Cisco IOS Software Modularity

**Cisco IOS Software**
The following is sample output from the `show registry` command using the `brief` keyword:

```
Router# show registry atm 3/0/0 brief
Registry objects: 1799 bytes: 213412
---
Registry 23: ATM Registry
Service 23/0:
  Service 23/1:
  Service 23/2:
  Service 23/3:
  Service 23/4:
  Service 23/5:
  Service 23/6:
  Service 23/7:
  Service 23/8:
  Service 23/9:
  Service 23/10:
  Service 23/11:
  Service 23/12:
  Service 23/13:
```
Service 23/14:

Registry 25: ATM routing Registry
Service 25/0:

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

### Table 164: show registry brief (Cisco IOS) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry objects</td>
<td>Number of objects in the registry.</td>
</tr>
<tr>
<td>bytes</td>
<td>Registry size, in bytes.</td>
</tr>
<tr>
<td>Registry</td>
<td>Displays the specified registry service number and type of registry service.</td>
</tr>
</tbody>
</table>

**Cisco IOS Software Modularity**

The following is partial sample output from the `show registry` command when running a software Modularity image:

```
Router# show registry
Registry information for ios-base:1:
####################################
AAA_ACCOUNTING : 11 services
 / 1 : List list[000]
 / 2 : List list[000]
 / 3 : Case size[020] list[000] default=0x7267C5D0 return
 / 4 : Case size[020] list[000] default=0x7267C5D0 return
 / 5 : Case size[020] list[000] default=0x7267C5D0 return
 / 6 : Case size[020] list[000] default=0x7267C5D0 return
 / 7 : Retval size[020] list[000] default=0x7267C5E4 return
 / 8 : Retval size[020] list[000] default=0x7267C5E4 return
 / 9 : Retval size[020] list[000] default=0x7267C5E4 return
 / 10: Stub 0x7267C5E4 return_zero
 / 11: Stub 0x76545BA0
AAA_ACCOUNTING : 11 services, 140 global bytes, 160 heap bytes
```

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

### Table 165: show registry (Software Modularity) Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry information</td>
<td>Displays the registry information by process name.</td>
</tr>
<tr>
<td>services</td>
<td>Number of services displayed.</td>
</tr>
<tr>
<td>global bytes</td>
<td>Number of bytes for the service,</td>
</tr>
</tbody>
</table>
### show reload

To display the reload status on the router, use the `show reload` command in EXEC mode.

```
show reload
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the `show reload` command to display a pending software reload. To cancel the reload, use the `reload cancel` privileged EXEC command.

**Examples**

The following sample output from the `show reload` command shows that a reload is schedule for 12:00 a.m. (midnight) on Saturday, April 20:

```
Router# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
Router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reloads the operating system.</td>
</tr>
</tbody>
</table>

### show resource-pool queue

To display resource pool and queue information about the router, use the `show resource-pool queue` command in user EXEC or privileged EXEC mode.

```
show resource-pool queue {description|statistics}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Displays information about the resource-pool queue description.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays information about the resource-pool queue statistics.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>) Privileged EXEC (#)
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show resource-pool queue` command to display the resource pool and queue information on the router.

**Examples**

The following is sample output from the `show resource-pool queue description` command. The field descriptions are self-explanatory.

```
Router# show resource-pool description
Resource-management call state description
State Description
--------------------------- -----------
RM_DNIS_AUTHOR : Waiting for DNIS author
RM_DNIS_AUTH_SUCCEEDED : Waiting for resource alloc
RM_DNIS_RES_ALLOCATED : Call established
RM_DNIS_REQ_IDLE : Disc while in RM_DNIS_AUTHOR/RM_DNIS_AUTH_SUCCEEDED
/RM_DNIS_REQ_IDLE_AUTHOR
RM_DNIS_REQ_IDLE_AUTHOR : New call while in RM_DNIS_REQ_IDLE
RM_RPM_RES_AUTHOR : Waiting for RPM author
RM_RPM_RES_ALLOCATING : Waiting for resource alloc
RM_RPM_RES_ALLOCATED : RPM call established
RM_RPM_AUTH_REQ_IDLE : Disc while in RM_RPM_RES_AUTHOR
/RM_RPM_AUTH_REQ_IDLE_AUTHOR
RM_RPM_RES_REQ_IDLE : Disc while in RM_RPM_RES_ALLOCATING
/RM_RPM_RES_REQ_IDLE_AUTHOR
RM_RPM_AUTH_REQ_IDLE_AUTHOR : New call while in RM_RPM_RES_REQ_IDLE
RM_RPM_DISCONNECTING : RPM initiates disconnect and is waiting for ack
RM_RPM_DISCONNECTING_AUTHOR : New call while in RM_RPM_DISCONNECTING
5400-XM-1#sh resource-pool queue stat
The following is sample output from the `show resource-pool queue statistics`command:
```
Router# show resource-pool statistics
Resource-management event queue information (queue depth 0)
Event In queue Total
--------------------------- ---------- ----------
DIALER_INCALL : 0 0
DIALER_DISCON : 0 0
GUARDTIMER_EXPIRY_EVENT : 0 0
RM_DNIS_AUTHOR_SUCCESS : 0 0
RM_DNIS_AUTHOR_FAIL : 0 0
RM_DNIS_RES_ALLOC_SUCCESS : 0 0
RM_DNIS_RES_ALLOC_FAIL : 0 0
RM_DNIS_RPM_REQUEST : 0 0
RM_RPM_RES_AUTHOR_SUCCESS : 0 0
RM_RPM_RES_AUTHOR_FAIL : 0 0
RM_RPM_RES_ALLOC_SUCCESS : 0 0
RM_RPM_RES_ALLOC_FAIL : 0 0
RM_RPM_DISC_ACK : 0 0
--------------------------- ---------- ----------
SUM : 0 0
Resource-management call information (0 active calls)
State Active Total
--------------------------- ---------- ----------
RM_DNIS_AUTHOR : 0 0
RM_DNIS_AUTH_SUCCEEDED : 0 0
RM_DNIS_RES_ALLOCATED : 0 0
```
show protocols through showmon

show rhosts

To display information about current remote hosts, use the `show rhosts` command in privileged EXEC mode.

**show rhosts**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS 2.1 XE</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show rhosts` command.

```
Router# show rhosts
Local user  Host/Access list     Remote user
tcp-scale-mcp1 12                tcp-scale-mcp2
tcp-scale-mcp1 12                tcp-scale-3
```

The following table describes the significant fields shown in the display.
Table 166: show rhosts Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local user</td>
<td>Displays the name of the user on the local router. This name gets communicated to the network administrator or to the user on the remote system.</td>
</tr>
<tr>
<td>Host/Access list</td>
<td>Displays the name or the IP address of the remote host from which the local router will accept remotely executed commands.</td>
</tr>
<tr>
<td>Remote user</td>
<td>Displays the name of the user on the remote host from which the router will accept remotely executed commands.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip rcmd remote-host</code></td>
<td>Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using RSH or RCP.</td>
</tr>
</tbody>
</table>

show rom-monitor

To show both the read-only and the upgrade ROM monitor (ROMMON) image versions and also the ROMMON image running on the Cisco 7200 VXR or Cisco 7301 router, use the `show rom-monitor` command in user EXEC, privileged EXEC, or diagnostic mode.

**Supported Platforms Other than the Cisco ASR1000 Series Routers**

`show rom-monitor`

**Cisco ASR 1000 Series Routers**

`show rom-monitor slot`

**Syntax Description**

<table>
<thead>
<tr>
<th>slot</th>
<th>Specifies the slot that contains the ROMMON. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>number</code> --The number of the SIP slot that requires the ROMMON upgrade.</td>
</tr>
<tr>
<td></td>
<td>• <code>F0</code> --Embedded Service Processor slot 0.</td>
</tr>
<tr>
<td></td>
<td>• <code>F1</code> --Embedded Service Processor slot 1.</td>
</tr>
<tr>
<td></td>
<td>• <code>FP active</code> --Active Embedded Service Processor.</td>
</tr>
<tr>
<td></td>
<td>• <code>FP standby</code> --Standby Embedded Service Processor.</td>
</tr>
<tr>
<td></td>
<td>• <code>R0</code> --Route Processor slot 0.</td>
</tr>
<tr>
<td></td>
<td>• <code>R1</code> --Route Processor slot 1.</td>
</tr>
<tr>
<td></td>
<td>• <code>RP active</code> --Active Route Processor.</td>
</tr>
<tr>
<td></td>
<td>• <code>RP standby</code> --Standby Route Processor.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>), Privileged EXEC (#), Diagnostic (diag)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(28)S</td>
<td>This command was introduced on the Cisco 7200 VXR router.</td>
</tr>
<tr>
<td>12.3(9)</td>
<td>This command was integrated into Cisco IOS Release 12.3(9) and implemented on the Cisco 7301 router.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(8)T.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Cisco IOS XE Release 2.1 | This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced:  
  - This command was introduced in diagnostic mode. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers.  
  - The *slot* argument was introduced. |
| 15.0(1)M | The command was modified on Cisco 1800 series routers. The output of the command was modified to let you know that the upgradable ROMMON version is not visible due to the license activity and reload is required. |

### Usage Guidelines

Use the `show rom-monitor` command when the router boots a Cisco IOS software image. In this case, the device prompt will be something like “Router>”. Use the `showmon` command when the device boot to Rom Monitor mode instead of booting a Cisco IOS image. In this case, the device prompt will be something like “rommon n >” where “n” is a number.

### Note

On Cisco 1800 series routers, the `show rom-monitor` command does not show the version of the upgradable ROMMON. To view the version of the upgradable ROMMON, you may need to reload the router while using the upgradable ROMMON image. If you are using the read-only ROMMON, then the upgradable ROMMON disappears. You need to run the `upgrade rom-monitor file` command for the upgradable ROMMON. Otherwise, the `upgrade rom-monitor preference upgrade` command is rejected with the message “No Upgrade ROMMON present, cannot select it.” During ROMMON bootup, if you are running upgradable ROMMON, then the ROMMON first displays the read-only ROMMON message, “Running new upgrade for first time.” This message is followed by the upgradable ROMMON message.

### Examples

The following sample output from the `show rom-monitor` command, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, displays both the ROMMON images and verifies that the upgrade ROMMON image is running:

```
Router> show rom-monitor
ReadOnly ROMMON version:
System Bootstrap, Version 12.2(20031011:151758)
Copyright (c) 2004 by Cisco Systems, Inc.
Upgrade ROMMON version:
System Bootstrap, Version 12.2(20031011:151758)
```
Currently running ROMMON from Upgrade region
ROMMON from Upgrade region is selected for next boot

The following is sample output from the show rom-monitor command in on Cisco 1800 series routers. To view the version of the upgradable ROMMON, you may need to reload the router while using the upgradable ROMMON image.

```
Router# show rom-monitor
ReadOnly ROMMON version:
System Bootstrap, Version 12.3(8r)YH3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2005 by cisco Systems, Inc.
Upgrade ROMMON version is not visible due to recent license activity,
such as license installation, removal, or the use of evaluation license
Reload is required to show the upgrade ROMMON version
Currently running ROMMON from Upgrade region
ROMMON from Upgrade region is selected for next boot

Router# reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.3(8r)YH3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2005 by cisco Systems, Inc.
Running new upgrade for first time
System Bootstrap, Version 12.3(8r)YH13, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2008 by cisco Systems, Inc.
C1800 platform with 262144 Kbytes of main memory with parity disabled
Upgrade ROMMON initialized

In the following example, the ROMMON image in RP 0 of a Cisco ASR 1006 router is verified using the show rom-monitor command:

```
Router# show rom-monitor r0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.

The fields in the examples are self-explanatory.

### show rom-monitor slot

To display the ROM monitor (ROMMON) status, use the `show rom-monitor` command in user EXEC or privileged EXEC mode.

```
show rom-monitor slot num {sp|rp}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>num</th>
<th>Displays the slot number of the ROMMON for which the status is to be displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sp</td>
<td>Displays the ROMMON status of the switch processor.</td>
</tr>
<tr>
<td>rp</td>
<td>Displays the ROMMON status of the route processor.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC Privileged EXEC
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was integrated into Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you enter the `show rom-monitor slot` command, the output displays the following:

- **Region region1 and region2**—Displays the status of the ROMMON image and the order of preference from which the region1 or region2 images should be booted. The ROMMON image status values are as follows:
  - First run—Indicates that a check of the new image is being run.
  - Invalid—Indicates that the new image has been checked and the upgrade process has started.
  - Approved—Indicates that the ROMMON field upgrade process has completed.
- **Currently running**—This field displays the currently running image and the region.

The `sp` or `rp` keyword is required only if a supervisor engine is installed in the specified slot.

### Examples

This example shows how to display ROMMON information:

Router# `show rom-monitor slot 1 sp`

Region F1: APPROVED
Region F2: FIRST_RUN, preferred
Currently running ROMMON from F1 region

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrade rom-monitor</td>
<td>Sets the execution preference on a ROMMON.</td>
</tr>
</tbody>
</table>

### show running identity policy

To display identity policy information, use the `show running identity policy` command in privileged EXEC mode.

```
show running identity policy [name]
```

**Syntax Description**

- `name` (Optional) Name of the identity policy.

**Command Modes**

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SX</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Examples

The following is output from the `show running identity policy` command:

```
Router# show running identity policy
Building configuration...
Current configuration:
  identity policy p1
    access-group some-acl
  identity policy p2
    access-group another-acl
    redirect url http://www.foo.com/bar.html match redirect-acl
end
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-configuration</td>
<td>Displays the running configuration for a router.</td>
</tr>
</tbody>
</table>

show running identity profile

To display identity profile information, use the `show running identity profile` command in privileged EXEC mode.

```
show running identity profile [{default|dot1x|eapoudp}]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>(Optional) Displays default identity profile information.</td>
</tr>
<tr>
<td>dot1x</td>
<td>(Optional) Displays 802.1x identity profile information.</td>
</tr>
<tr>
<td>eapoudp</td>
<td>(Optional) Displays EAPoUDP identity profile information.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SX</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following is output from the `show running identity profile` command:

```
Router# show running identity profile
Building configuration...
Current configuration:
  identity profile default
    device authorize type cisco ip phone
  identity profile eapoudp
    device authorize ip-address 10.0.0.0 255.0.0.0 policy p1
  identity profile dot1x
    device authorize mac-address 0001.0203.0405 ffff.ffff.ffff policy p2
end
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-configuration</td>
<td>Displays the running configuration for a router.</td>
</tr>
</tbody>
</table>

**show running-config**

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the `show running-config` command in privileged EXEC mode.

```plaintext
show running-config [options]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>options</th>
<th>(Optional) Keywords used to customize output. You can enter more than one keyword.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• all</td>
<td>--Expands the output to include the commands that are configured with default parameters. If the all keyword is not used, the output does not display commands configured with default parameters.</td>
</tr>
<tr>
<td>• brief</td>
<td>--Displays the configuration without certification data and encrypted filter details. The brief keyword can be used with the <code>linenum</code> keyword.</td>
</tr>
<tr>
<td>• class-map [name][linenum]</td>
<td>--Displays class map information. The <code>linenum</code> keyword can be used with the <code>class-map name</code> option.</td>
</tr>
<tr>
<td>• control-plane [cef-exception host transit]</td>
<td>--Displays control-plane information. The <code>cef-exception</code>, <code>host</code>, and <code>transit</code> keywords can be used with the <code>control-plane</code> option.</td>
</tr>
<tr>
<td>• flow {exporter</td>
<td>monitor</td>
</tr>
<tr>
<td>• full</td>
<td>--Displays the full configuration.</td>
</tr>
<tr>
<td>• interface type number</td>
<td>--Displays interface-specific configuration information. If you use the <code>interface</code> keyword, you must specify the interface type and the interface number (for example, <code>interface ethernet 0</code>). Keywords for common interfaces include async, ethernet, fastEthernet, group-async, loopback, null, serial, and virtual-template. Use the `show run interface ?command to determine the interfaces available on your system.</td>
</tr>
<tr>
<td>• linenum</td>
<td>--Displays line numbers in the output. The brief or full keyword can be used with the <code>linenum</code> keyword. The <code>linenum</code> keyword can be used with the <code>class-map</code>, <code>interface</code>, <code>map-class</code>, <code>policy-map</code>, and <code>vc-class</code> keywords.</td>
</tr>
<tr>
<td>• map-class [atm</td>
<td>dialer</td>
</tr>
</tbody>
</table>
- **partition types** -- Displays the configuration corresponding to a partition. The `types` keyword can be used with the `partition` option.

- **policy-map [name] [linenum]** -- Displays policy map information. The `linenum` keyword can be used with the `policy-map name` option.

- **vc-class [name] [linenum]** -- Displays VC-class information (the display is available only on certain devices such as the Cisco 7500 series devices). The `linenum` keyword can be used with the `vc-class name` option.

- **view full** -- Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view.

- **vrf name** -- Displays the Virtual routing and forwarding (VRF)-aware configuration module number.

- **vlan [vlan-id]** -- Displays the specific VLAN information; valid values are from 1 to 4094.

---

**Command Default**

The default syntax, `show running-config`, displays the contents of the running configuration file, except commands configured using the default parameters.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>This command was replaced by the <code>more system:running-config</code> command.</td>
</tr>
<tr>
<td>12.0(1)T</td>
<td>This command was integrated into Cisco IOS Release 12.0(1)T, and the output modifier (</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>This command was modified. The <code>linenum</code> keyword was added.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was modified. The <code>view full</code> option was added.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)SX. The <code>module number</code> and <code>vlan vlan-id</code> keywords and arguments were added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SX</td>
<td>This command was integrated into Release 12.2(17d)SXB and implemented on the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was modified. The <code>all</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2. This command was enhanced to display the configuration information for traffic shaping overhead accounting for ATM and was implemented on the Cisco 10000 series device for the PRE3.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was modified. Support for the Cisco 7300 series device was added.</td>
</tr>
</tbody>
</table>
Modification Release

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The <strong>partition</strong> and <strong>vrf</strong> keywords were added. The <strong>module</strong> and <strong>vlan</strong> keywords were removed.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The output was modified to include encrypted filter information.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was modified. The output was modified to display Access Control List (ACL) information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface serial 2/1 linenum | begin 3**. To display the output modifiers that are available for a keyword, enter | ? after the keyword. Depending on the platform you are using, the keywords and the arguments for the **options** argument may vary.

Prior to Cisco IOS Release 12.2(33)SXH, the **show running-config** command output omitted configuration commands set with default values. Effective with Cisco IOS Release 12.2(33)SXH, the **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: cdp holdtime 180.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all** commands is the same; that is, the configured parameter is displayed.

**Note**

In Cisco IOS Release 12.2(33)SXH, the **all** keyword expands the output to include some of the commands that are configured with default values. In subsequent Cisco IOS releases, additional configuration commands that are configured with default values will be added to the output of the **show running-config all** command.

Effective with Cisco IOS Release 12.2(33)SXI, the **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list** command.

**Cisco 7600 Series Device**

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** command. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command displays the
operating mode of an interface, and the **show running-config** command displays the configured mode of the interface.

The **show running-config** command output for an interface might display the duplex mode but no configuration for the speed. This output indicates that the interface speed is configured as auto and that the duplex mode that is displayed becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode that is displayed with the **show running-config** command.

### Examples

The following example shows the configuration for serial interface 1. The fields are self-explanatory.

```
Device# show running-config interface serial 1
Building configuration...
Current configuration:
!
interface Serial1
   no ip address
   no ip directed-broadcast
   no ip route-cache
   no ip mroute-cache
   shutdown
end
```

The following example shows the configuration for Ethernet interface 0/0. Line numbers are displayed in the output. The fields are self-explanatory.

```
Device# show running-config interface ethernet 0/0 linenum
Building configuration...
Current configuration : 104 bytes
1 : !
2 : interface Ethernet0/0
3 : ip address 10.4.2.63 255.255.255.0
4 : no ip route-cache
5 : no ip mroute-cache
6 : end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Device# show running-config linenum | begin 10

10 : boot-start-marker
11 : boot-end-marker
12 : !
13 : no logging buffered
14 : enable password ####
15 : !
16 : spe 1/0 1/7
17 : firmware location bootflash:mica-modem-pw.172.16.0.0.bin
18 : !
19 : !
20 : resource-pool disable
21 : !
22 : no aaa new-model
23 : ip subnet-zero
24 : ip domain name cisco.com
25 : ip name-server 172.16.11.48
26 : ip name-server 172.16.2.133
27 : !
```
The following example shows how to display the module and status configuration for all modules on a Cisco 7600 series device. The fields are self-explanatory.

Device# show running-config
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname device
!
boot buffersize 126968
boot system flash slot0:7600r
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin
enable password lab
!
clock timezone Pacific -8
clock summer-time Daylight recurring
redundancy
  main-cpu
    auto-sync standard
!
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 200 forward-time 21
port-channel load-balance sdip
!
!
  shutdown
!
!
!
!

In the following sample output from the show running-config command, the shape average command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory.
Device# show running-config

subscribers policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync

controller T1 2/0
framing sf
linecode ami

controller T1 2/1
framing sf
linecode ami

policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
The following is sample output from the show running-config class-map command. The fields in the display are self-explanatory.

Device# show running-config class-map
Building configuration...
Current configuration : 2910 bytes
!
class-map type stack match-all ip_tcp_stack
match field IP protocol eq 0x6 next TCP

class-map type access-control match-all my
match encrypted
filter-version 0.1, Dummy Filter 2
filter-id 123
algorithm aes256cbc
cipherkey realm-cisco.sym
ciphervalue #

exit

class-map type stack match-all ip_udp_stack
match field IP protocol eq 0x11 next UDP

class-map type access-control match-all psirt1
match encrypted
filter-version 0.0 DummyVersion_20090101_1830
filter-id cisco-sa-20090101-dummy_dcts_001
filter-hash F6C50BED10521002B8A170F29AF059C53
algorithm aes256cbc
cipherkey realm-cisco.sym
ciphervalue #

exit

match start TCP payload-start offset 0 size 10 regex "abc.*def"
match field TCP source-port eq 1234
class-map type access-control match-all psirt2
    match encrypted
    filter-version 0.0_DummyVersion_20090711_1830
    filter-id cisco-sa-20090711-dummy_ddts_002
    filter-hash DE0EB7D3C4AFDD990038174A472E4709
    algorithm aes256cbc
    cipherkey realm-cisco.sym

The following example shows that the teletype (tty) line 2 is reserved for communicating with the 2nd core:

Device# show running
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
interface Ethernet0
  ip address 172.25.213.150 255.255.255.128
  no ip directed-broadcast
  no logging event link-status
!
interface Serial0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
  no fair-queue
!
interface Serial1
  no ip address
  no ip directed-broadcast
  shutdown
!
ip default-gateway 172.25.213.129
ip classless
ip route 0.0.0.0 0.0.0.0 172.25.213.129
!
!
line con 0
  transport input none
line 1 6
  no exec
  transport input all
line 7
  no exec
  exec-timeout 300 0
  transport input all
line 8 9
  no exec
```
transport input all
line 10
  no exec
transport input all
stopbits 1
line 11 12
  no exec
transport input all
line 13
  no exec
transport input all
speed 115200
line 14 16
  no exec
transport input all
line aux 0
line vty 0 4
  password cisco
login
end
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.</td>
<td></td>
</tr>
<tr>
<td>boot config</td>
<td>Specifies the device and filename of the configuration file from which the device configures itself during initialization (startup).</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration. (Command alias for the <code>copy system:running-config nvram:startup-config</code> command.)</td>
<td></td>
</tr>
<tr>
<td>shape</td>
<td>Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.</td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays statistics for all interfaces configured on the device or access server.</td>
<td></td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps, and displays ATM overhead accounting information, if configured.</td>
<td></td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the <code>CONFIG_FILE</code> environment variable. (Command alias for the <code>more:nvram startup-config</code> command.)</td>
<td></td>
</tr>
</tbody>
</table>

**show running-config control-plane**

To display the control plane information for the running configuration, use the `show running-config control-plane` command in privileged EXEC mode.

```
show running-config control-plane [{cef-exception|host|transit}]
```
show running-config control-plane

The following is sample output from the `show running-config control-plane` command. The field descriptions are self-explanatory.

```
Router# show running-config control-plane
Building configuration...
Current configuration : 14 bytes
!
control-plane
!
end
```

**show running-config map-class**

To display only map-class configuration information from the running configuration file, use the `show running-config map-class` command in privileged EXEC mode.

```
show running-config map-class [{atm [map-class-name]}|dialer [map-class-name]|frame-relay [map-class-name]] [linenum]
```

**Syntax Description**

- **atm** (Optional) Displays only ATM map-class configuration lines.
- **dialer** (Optional) Displays only dialer map-class configuration lines.
- **frame-relay** (Optional) Displays only Frame Relay map-class configuration lines.
- **map-class-name** (Optional) Displays only configuration lines for the specified map-class.
- **linenum** (Optional) Displays line numbers in the output.
**Command Default**
Displays all map-class configuration in the running configuration file.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>The <code>map-class</code> extension to the <code>show running-config</code> command was introduced to show only lines pertaining to dialer or Frame Relay map classes.</td>
</tr>
<tr>
<td>12.1(2)T</td>
<td>The <code>atm</code>, <code>dialer</code>, and <code>frame-relay</code> keywords and <code>map-class-name</code> argument were introduced.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>The <code>linenum</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `show running-config map-class` command to display the following information from the running configuration file:

- All map classes configured on the router.
- Map classes configured specifically for ATM, Frame Relay, or dialer.
- A specific ATM, Frame Relay, or dialer map class.

Use the `linenum` keyword to display line numbers in the output. This option is useful for identifying a particular portion of a very large configuration.

**Examples**

**All Map Classes Configured on the Router Example**
The following example displays all map classes configured on the router:

```
Router# show running-config map-class
Building configuration...
Current configuration:
!
map-class frame-relay cir60
  frame-relay bc 16000
  frame-relay adaptive-shaping becn
!
map-class frame-relay cir70
  no frame-relay adaptive-shaping
  frame-relay priority-group 2
!
map-class atm vc100
  atm aal5mux
!
map-class dialer dialer1
  dialer idle-timeout 10
end
```

**All Frame Relay Map Classes Example**
The following example displays all Frame Relay map classes on the router:
Router# show running-config map-class frame-relay

Building configuration...
Current configuration:
!
map-class frame-relay cir60
frame-relay bc 16000
frame-relay adaptive-shaping becn
!
map-class frame-relay cir70
no frame-relay adaptive-shaping
frame-relay priority-group 2
end

A Specific Map Class and Display of Line Numbers Example

The following example displays a specific map class called class1. Line numbers are displayed in the output.

Router# show running-config map-class frame-relay class1 linenum

Building configuration...
Current configuration:
1 : !
2 : map-class frame-relay boy
3 : no frame-relay adaptive-shaping
4 : frame-relay cir 1000
5 : end

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>map-class atm</td>
<td>Specifies the ATM map class for an SVC.</td>
</tr>
<tr>
<td>map-class dialer</td>
<td>Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.</td>
</tr>
<tr>
<td>map-class frame-relay</td>
<td>Specifies a map class to define QoS values for a Frame Relay VC.</td>
</tr>
<tr>
<td>more system:running-config</td>
<td>Displays contents of the currently running configuration file (equivalent to the show running-config command.)</td>
</tr>
</tbody>
</table>

show running-config partition

To display the list of commands that make up the current running configuration for a specific part of the system’s global running configuration, use the show running-config partition command in privileged EXEC mode.

show running-config partition part
The `part` argument will consist of one or more keyword options. These keywords represent a partition of the system’s running configuration state, as a major-descriptor and, in some cases, one or more minor-descriptors.

For example, in the command `show running-config partition router eigrp 1`, the major-descriptor for the `part` argument is the `router` keyword, and the minor-descriptors for the `part` argument are the `eigrp 1` keywords.

The actual list of `part` keyword options will depend on your system hardware, what feature set you are running, and what features are currently configured on your system.

Some examples of command `part` keyword options are provided here for reference. Use the `show running-config partition ?` command on your system to view the list of command options available on your system.

- **access-list** -- Displays all running configuration commands that make up the access-list configuration partition.
- **boot** -- Displays all running configuration commands that make up the boot configuration partition.
- **class-map** -- Displays all running configuration commands that make up the class-map configuration partition.
- **global-cdp** -- Displays all running configuration commands that make up the global CDP configuration partition.
- **interface [type slot/port/number]** -- Displays all running configuration commands that make up the interfaces configuration partition or the configuration commands that are applied to the specified interface.
- **line** -- Displays all running configuration commands that make up the line command configuration partition.
- **policy-map** -- Displays all running configuration commands that make up the policy-map configuration partition.
- **route-map** -- Displays all running configuration commands that make up the route-map configuration partition.
- **router [protocol]** -- Displays all running configuration commands that make up the router configuration partition, or the configuration commands for the specified routing protocol.
- **service** -- Displays all running configuration commands that make up the services (small server) configuration partition.
- **snmp** -- Displays all running configuration commands that make up the SNMP configuration partition.
- **|** - Allows for the addition of output modifiers.

### Command Default

None

### Command Modes

Privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRB</td>
<td>This command was introduced for Cisco 7600 series images in Cisco IOS Release 12.2SR as part of the “Configuration Partitioning” feature.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the Configuration Partitioning feature is enabled, the system groups the configuration state of the device into parts (called “partitions”) for the purpose of generating the virtual running configuration file (the list of configuration commands). The selective processing of the system’s configuration state for the purpose of generating a partial running configuration is called “configuration partitioning.”

This command is not related to hard drive or flash drive partitioning.

This granular access to configuration information offers important performance benefits for high-end routing platforms with very large configuration files, as the system wide generation of a complete virtual configuration file from all components on systems with large and complex configurations can become overly resource intensive and be unacceptably slow.

The `show running-config partition` command allows you to display only the part of the running configuration that you want to examine, while also allowing the system to process only the collection of system components (such as specific interfaces) that you need to display. This is in contrast to other existing extensions to the `show running-config` command, which only filter the generated list after all system components have been processed.

The Configuration Partitioning feature is enabled by default in Cisco IOS software images that support the feature. To disable the feature, use the `no parser config partition` command.

Examples

In the following example, the system generates a view of the running configuration by polling only the components associated with the access-list parts of the running configuration state, and then displays only those access-list-related configuration commands.

```
Router# show running-config partition access-list
Building configuration...
Current configuration : 127 bytes
!
Configuration of Partition access-list
!
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
!
end
```

In the following example, only the main configuration partition associated with the interface configuration is queried, and only the configuration commands associated with Fast Ethernet interface 0/1 are displayed.

```
Router# show running-config partition interface fastethernet0/1
Building configuration...
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config</td>
<td>Copies the running configuration to the default startup configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays statistics for all interfaces configured on the router or access server.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Generates and displays a virtual configuration file that lists all configuration commands that are in effect on the system.</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the more:nvram startup-config command.)</td>
</tr>
</tbody>
</table>

**show scp**

To display Switch-Module Configuration Protocol (SCP) information, use the `show scp` in privileged EXEC mode on the Switch Processor.

```
show scp {accounting|counters|linecards [details]|mcast {group group-id|inst}|process id|status}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Displays information about the SCP accounting.</td>
</tr>
<tr>
<td>counters</td>
<td>Displays information about the SCP counter.</td>
</tr>
<tr>
<td>linecards</td>
<td>Displays information about the Optical Services Module (OSM) wide area network (WAN) modules in the chassis.</td>
</tr>
<tr>
<td>details</td>
<td>(Optional) Displays detailed information about the OSM WAN module.</td>
</tr>
<tr>
<td>mcast</td>
<td>Displays information about the SCP multicast.</td>
</tr>
<tr>
<td>group group-id</td>
<td>(Optional) Displays information for a specific group and group ID; valid values are from 1 to 127.</td>
</tr>
<tr>
<td>inst</td>
<td>(Optional) Displays information for an instance.</td>
</tr>
</tbody>
</table>
**show scp**

<table>
<thead>
<tr>
<th><strong>process</strong></th>
<th><strong>id</strong></th>
<th>Displays all the processes that have registered an SAP with SCP.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>status</strong></td>
<td></td>
<td>Displays information about the local SCP server status.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC on the Switch Processor

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>The output of the <code>show scp process</code> command was changed to display all the processes that have registered an SAP with SCP on the Supervisor Engine 720 only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>The output of the <code>show scp status</code> command was changed to additionally display the Flow Control State (FC-State) and the Flow Control Count (FC-Count).</td>
</tr>
</tbody>
</table>

**Examples**

This example displays the SCP flow control status:

```
Router# show scp status
Rx 185, Tx 181, scp_my_addr 0x14
Id Sap Channel name current/peak/retry/dropped/totaltime(queue/process/ack) FC-state
FC-count
-------------------------------------------------------------- --------- ---- ------- ------ ------- ------ -------
0 18 SCP Unsolicited:18 801/ 0/0/ 0/ 0/ 0/ 0/ 0 off 0
1 80 SCP Unsolicited:80 0/ 0/0/ 0/ 0/ 0/ 0/ 0 off 0
2 23 SCP async: LCP#5 0/ 0/0/ 0/ 0/ 0/ 0/ 0 off 0
3 0 SCP Unsolicited:0 0/ 1/0/ 0/ 5 0/ 0/ 0/ 0 off 0
--------------------------------------------------------------------------------------------------------------------------
```

FC-state indicates the flow control state and FC-count indicates the number of times flow control has been turned on.

This example shows how to display all the processes that have registered an SAP with SCP:

```
Router# show module
Mod Ports Card Type Model Serial No.
--- ----- ------------------------ ------------------ -----------
1 48 48-port 10/100 mb RJ45 WS-X6148-RJ-45 SAL091800RY
2 0 2 port adapter Enhanced FlexWAN WS-X6582-2PA JAE0940MH7Z
3 8 8 port 1000mb GBIC Enhanced GoS WS-X6408A-GBIC SAL09391KZH
5 2 Supervisor Engine 720 (Active) WS-SUP720-3BXL SAL0937UE6
6 2 Supervisor Engine 720 (Hot) WS-SUP720-3BXL SAL09148P59
Mod MAC addresses Hw Fw Sw Status
--- ---------------------------------- ------ ---------- ----------
1 0013.c3f8.d2c4 to 0013.c3f8.d2f3 5.0 8.3(1) 8.6(0.366)TA Ok
2 0015.2bc3.5b40 to 0015.2bc3.5b7f 2.1 12.2(nightly 12.2(nightly Ok
3 0015.6324.ed48 to 0015.6324.ed4f 3.1 5.4(2) 8.6(0.366)TA Ok
5 0014.a97d.b0ac to 0014.a97d.b0af 4.3 8.4(2) 12.2(nightly Ok
6 0013.7f0d.0660 to 0013.7f0d.0663 4.3 8.4(2) 12.2(nightly Ok
```
### show slot

To display information about the PCMCIA flash memory cards file system, use the `show slot` command in user EXEC or privileged EXEC mode.

```
show slot [ {all|chips|detailed|err|summary} ]
```

#### Syntax Description

- **all**
  (Optional) Displays all possible flash system information for all PCMCIA flash cards in the system.

- **chips**
  (Optional) Displays flash chip information.

- **detailed**
  (Optional) Displays the flash detailed directory.

- **err**
  (Optional) Displays the flash chip erase and write retries.

- **summary**
  (Optional) Displays the flash partition summary.

#### Command Modes

- User EXEC Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the `show slot` command to display details about the files in a particular linear PCMCIA flash memory card of less than 20 MB and some 32 MB linear PCMCIA cards.
Use the `show disk` command for ATA PCMCIA cards. Other forms of this commands are `show disk0:` and `show disk1:`.

For more information regarding filesystems and flash cards, access the *PCMCIA Filesystem Compatibility Matrix and Filesystem Information* document at the following URL:


To see which flash cards are used in your router, use the `show version` command and look at the bottom portion of the output.

The following display indicates an ATA PCMCIA flash disk.

```
Router# show version
.
46976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
```

The following display indicates a linear PCMCIA flash card with 20480K bytes of flash memory in card at slot 1 with a sector size of 128K.

```
Router# show version
.
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
```

In some cases the `show slot` command will not display the file systems, use `show slot0:` or `show slot1:`.

The following example displays information about slot 0. The output is self-explanatory.

```
Router# show slot
PCMCIA Slot0 flash directory:
File  Length  Name/status
   1 11081464  c3660-bin-mz.123-9.3.P15
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

The following example shows all possible flash system information for all PCMCIA flash cards in the system.

```
Router# show slot all
Partition  Size    Used    Free    Bank-Size  State      Copy Mode
   1   20223K   10821K  9402K    4096K      Read/Write Direct
PCMCIA Slot0 flash directory:
File  Length  Name/status
    addr  fcksum  ccksum
   1 11081464  c3660-bin-mz.123-9.3.P15
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

```
Chip   Bank   Code   Size   Name
   1    1   89A0   2048KB INTEL 28F016SA
   2    1   89A0   2048KB INTEL 28F016SA
```
The following example shows flash chip information:

```
Router# show slot chips
```

<table>
<thead>
<tr>
<th>Chip</th>
<th>Bank</th>
<th>Code</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>89A0</td>
<td>2048KB</td>
<td>INTEL 28F016SA</td>
</tr>
</tbody>
</table>

The following example shows the flash detailed directory:

```
Router# show slot detailed
```

```
PCMCIA Slot0 flash directory:
File Length Name/status
addr fcksum ccksum
date
```

```
1 11081464 c3660-bin-mz.123-9.3.P15b
0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
```

```
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

The following example shows the flash chip erase and write retries:

```
Router# show slot err
```

```
PCMCIA Slot0 flash directory:
File Length Name/status
addr fcksum ccksum
date
```

```
1 11081464 c3660-bin-mz.123-9.3.P15b
0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
```

```
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

The following example shows the flash partition summary:

```
Router# show slot summary
```

```
Partition Size Used Free Bank-Size State Copy Mode
```

```
```
show slot0:

To display information about the PCMCIA flash memory card’s file system located in slot 0, use the show slot0: command in user EXEC or privileged EXEC mode.

show slot0: [{all | chips | detailed | err | summary}]

**Syntax Description**

- **all** (Optional) Displays all possible flash system information for all PCMCIA flash cards in the system.
- **chips** (Optional) Displays flash chip information.
- **detailed** (Optional) Displays the flash detailed directory.
- **err** (Optional) Displays the flash chip erase and write retries.
- **summary** (Optional) Displays the flash partition summary.

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the show slot0: command to display details about the files in a particular linear PCMCIA flash memory card of less than 20 MB and some 32 MB linear PCMCIA cards.

**Note**

Use the show disk command for ATA PCMCIA cards. Other forms of this commands are show disk0: and show disk1:
For more information regarding file systems and flash cards, access the *PCMCIA Filesystem Compatibility Matrix and Filesystem Information* document at the following URL:


To see which flash cards are used in your router, use the `show version` command and look at the bottom portion of the output.

The following display indicates an ATA PCMCIA flash disk.

```
Router# show version
.
46976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
```

The following display indicates a linear PCMCIA flash card with 20480K bytes of flash memory in card at slot 1 with a sector size of 128K.

```
Router# show version
.
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
```

**Note**

In some cases the `show slot` command will not display the file systems, use `show slot0: all` or `show slot1: all`.

**Examples**

The following example displays information about slot 0. The output is self-explanatory.

```
Router# show slot0:
PCMCIA Slot0 flash directory:
File Length Name/status
  1 11081464 c3660-bin-mz.123-9.3.P15b
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Router# show slot0: all
Partition Size Used Free Bank-Size State Copy Mode
  1 20223K 10821K 9402K 4096K Read/Write Direct
PCMCIA Slot0 flash directory:
File Length Name/status
addr fcksum ccksum
  1 11081464 c3660-bin-mz.123-9.3.P15b
  0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Chip Bank Code Size Name
  1 1 89A0 2048KB INTEL 28F016SA
  2 1 89A0 2048KB INTEL 28F016SA
  1 2 89A0 2048KB INTEL 28F016SA
  2 2 89A0 2048KB INTEL 28F016SA
  1 3 89A0 2048KB INTEL 28F016SA
  2 3 89A0 2048KB INTEL 28F016SA
  1 4 89A0 2048KB INTEL 28F016SA
  2 4 89A0 2048KB INTEL 28F016SA
  1 5 89A0 2048KB INTEL 28F016SA
  2 5 89A0 2048KB INTEL 28F016SA
```

The following example shows flash chip information.

```
Router# show slot0: chips
```
The following example shows the flash detailed directory.

```
Router# show slot0: detailed
PCMCIA Slot0 flash directory:
File Length Name/status
  addr fcksum ccksum
  1 11081464 c3660-bin-mz.123-9.3.P15b
    0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

The following example shows the flash chip erase and write retries.

```
Router# show slot0: err
PCMCIA Slot0 flash directory:
File Length Name/status
  addr fcksum ccksum
  1 11081464 c3660-bin-mz.123-9.3.P15b
    0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

The following example shows the flash partition summary.

```
Router# show slot0: summary
Partition Size Used Free Bank-Size State Copy Mode
  1 20223K 10821K 9402K 4096K Read/Write Direct
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```
show slot1:

To display information about the PCMCIA flash memory card’s file system located in slot 1, use the `show slot1:` command in user EXEC or privileged EXEC mode.

```
show slot1: [all|chips|detailed|err|summary]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Displays all possible flash system information for all PCMCIA flash cards in the system.</td>
</tr>
<tr>
<td>chips</td>
<td>(Optional) Displays flash chip information.</td>
</tr>
<tr>
<td>detailed</td>
<td>(Optional) Displays the flash detailed directory.</td>
</tr>
<tr>
<td>err</td>
<td>(Optional) Displays the flash chip erase and write retries.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the flash partition summary.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show slot1:` command to display details about the files in a particular linear PCMCIA flash memory card of less than 20 MB and some 32 MB linear PCMCIA cards located in slot 1.

Use the `show disk` command for ATA PCMCIA cards. Other forms of this commands are `show disk0:` and `show disk1:`.

For more information regarding file systems and flash cards, access the *PCMCIA Filesystem Compatibility Matrix and Filesystem Information* document at the following URL:


To see which flash cards are used in your router, use the `show version` command and look at the bottom portion of the output.

The following display indicates an ATA PCMCIA flash disk.

```
Router# show version
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show slot1:</td>
<td>Displays information about the PCMCIA flash memory card’s file system located in slot 1.</td>
</tr>
<tr>
<td>show slot</td>
<td>Displays information about the PCMCIA flash memory cards.</td>
</tr>
</tbody>
</table>
The following display indicates a linear PCMCIA flash card with 20480K bytes of flash memory in card at slot 1 with a sector size of 128K.

Router# show version

20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).

In some cases the show slot command will not display the file systems. Use show slot0: or show slot1:.

Examples

The following example displays information about slot 0 using the slot0: command form. The output is self-explanatory.

Router# show slot0:

PCMCIA Slot0 flash directory:
File Length Name/status
1 11081493 c3660-bin-mz.123-9.3.PI5b
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Router# show slot0: all

Partition Size Used Free Bank-Size State Copy Mode
1 20222K 10821K 9402K 4096K Read/Write Direct

PCMCIA Slot0 flash directory:
File Length Name/status
addr fcksum ccksum
1 11081464 c3660-bin-mz.123-9.3.PI5b
0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Chip Bank Code Size Name
1 1 89A0 2048KB INTEL 28F016SA
1 2 89A0 2048KB INTEL 28F016SA
1 3 89A0 2048KB INTEL 28F016SA
1 4 89A0 2048KB INTEL 28F016SA
1 5 89A0 2048KB INTEL 28F016SA
2 1 89A0 2048KB INTEL 28F016SA
2 2 89A0 2048KB INTEL 28F016SA
2 3 89A0 2048KB INTEL 28F016SA
2 4 89A0 2048KB INTEL 28F016SA
2 5 89A0 2048KB INTEL 28F016SA

The following example shows flash chip information.

Router# show slot0: chips

20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Chip Bank Code Size Name
1 1 89A0 2048KB INTEL 28F016SA
1 2 89A0 2048KB INTEL 28F016SA
1 3 89A0 2048KB INTEL 28F016SA
1 4 89A0 2048KB INTEL 28F016SA
1 5 89A0 2048KB INTEL 28F016SA
2 1 89A0 2048KB INTEL 28F016SA
2 2 89A0 2048KB INTEL 28F016SA
2 3 89A0 2048KB INTEL 28F016SA
2 4 89A0 2048KB INTEL 28F016SA
2 5 89A0 2048KB INTEL 28F016SA
The following example shows the flash detailed directory.

Router# show slot1: detailed
PCMCIA Slot0 flash directory:
File Length Name/status
addr fcksum ccksum
 1 11081464 c3660-bin-mz.123-9.3.P15b
     0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
2048K bytes of processor board PCMCIA Slot0 flash (Read/Write)

The following example shows the flash chip erase and write retries.

Router# show slot1: err
PCMCIA Slot0 flash directory:
File Length Name/status
addr fcksum ccksum
 1 11081464 c3660-bin-mz.123-9.3.P15b
     0x40 0x5EA3 0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
2048K bytes of processor board PCMCIA Slot0 flash (Read/Write)

The following example shows the flash partition summary.

Router# show slot1: summary
Partition Size Used Free Bank-Size State Copy Mode
 1 20223K 10821K 9402K 4096K Read/Write Direct
2048K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir slot0:</td>
<td>Directory listing of files on a PCMCIA Flash card located in slot0.</td>
</tr>
<tr>
<td>dir slot1:</td>
<td>Directory listing of files on a PCMCIA Flash card located in slot1.</td>
</tr>
<tr>
<td>show slot0:</td>
<td>Displays information about the PCMCIA flash memory card’s file system located in slot 0.</td>
</tr>
<tr>
<td>show slot</td>
<td>Displays information about the PCMCIA flash memory cards.</td>
</tr>
</tbody>
</table>

show software authenticity file

To display information related to software authentication for a specific image file, use the show software authenticity file command in privileged EXEC mode.
show software authenticity file
{flash0:filename|flash1:filename|flash:filename|nvram:filename|usbflash0:filename|usbflash1:filename}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash0:</td>
<td>Displays information related to software authentication for flash 0 resources.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of the filename in memory.</td>
</tr>
<tr>
<td>flash1:</td>
<td>Displays information related to software authentication for flash 1 resources.</td>
</tr>
<tr>
<td>flash:</td>
<td>Displays information related to software authentication for flash resources.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Displays information related to software authentication for NVRAM resources.</td>
</tr>
<tr>
<td>usbflash0:</td>
<td>Displays information related to software authentication for Universal Serial Bus (USB) flash 0 resources.</td>
</tr>
<tr>
<td>usbflash1:</td>
<td>Displays information related to software authentication for USB flash 1 resources.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced for the Cisco 1941, 2900, and 3900 routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information.

Examples

The following example displays software authentication related information for an image file named c3900-universalk9-mz.SSA:

```
Router# show software authenticity file flash0:c3900-universalk9-mz.SSA
File Name : flash0:c3900-universalk9-mz.SSA
Image type : Development
  Signer Information
    Common Name : xxx
    Organization Unit : xxx
    Organization Name : xxx
    Certificate Serial Number : xxx
    Hash Algorithm : SHA512
    Signature Algorithm : 2048-bit RSA
    Key Version : A
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Name of the filename in the memory. For example, flash0:c3900-universalk9-mz.SSA refers to filename c3900-universalk9-mz.SSA in flash memory (flash0:).</td>
</tr>
</tbody>
</table>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image type</td>
<td>Displays the type of image.</td>
</tr>
<tr>
<td>Signer Information</td>
<td>Signature information.</td>
</tr>
<tr>
<td>Common Name</td>
<td>Displays the name of the software manufacturer.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Displays the hardware the software image is deployed on.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Displays the owner of the software image.</td>
</tr>
<tr>
<td>Certificate Serial Number</td>
<td>Displays the certificate serial number for the digital signature.</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>Displays the type of hash algorithm used in digital signature verification.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Displays the type of signature algorithm used in digital signature verification.</td>
</tr>
<tr>
<td>Key Version</td>
<td>Displays the key version used for verification.</td>
</tr>
</tbody>
</table>

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show software authenticity keys</td>
<td>Displays the software public keys that are in the storage with the key types.</td>
</tr>
<tr>
<td>show software authenticity running</td>
<td>Displays information related to software authentication for the current ROMMON, monitor library (monlib), and Cisco IOS image used for booting.</td>
</tr>
</tbody>
</table>

## show software authenticity keys

To display the software public keys that are in the storage with the key types, use the `show software authenticity keys` command in privileged EXEC mode.

```
Router# show software authenticity keys
```

### Syntax Description

This command has no argument or keywords.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced for the Cisco 1941, 2900, and 3900 routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The display from this command includes the public keys that are in the storage with the key types.

### Examples

The following is sample output from the `show software authenticity keys` command:

```
Router# show software authenticity keys
Public Key #1 Information
```
The following table describes the significant fields shown in the display.

### Table 168: show software authenticity running Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Key #</td>
<td>Public key number.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Displays the key type used for image verification.</td>
</tr>
<tr>
<td>Public Key Algorithm</td>
<td>Displays the name of the algorithm used for public key cryptography.</td>
</tr>
<tr>
<td>Modulus</td>
<td>Modulus of the public key algorithm.</td>
</tr>
<tr>
<td>Exponent</td>
<td>Exponent of the public key algorithm</td>
</tr>
<tr>
<td>Key Version</td>
<td>Displays the key version used for verification.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show software authenticity file</td>
<td>Displays information related to software authentication for the loaded image file.</td>
</tr>
<tr>
<td>show software authenticity running</td>
<td>Displays information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting.</td>
</tr>
</tbody>
</table>

### show software authenticity running

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the **show software authenticity running** command in privileged EXEC mode.

**show software authenticity running**
Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced for the Cisco 1941, 2900, and 3900 routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The information displayed by the show software authenticity running command about the current ROMMON, monlib and Cisco IOS image used for booting includes:

- Image credential information
- Key type used for verification
- Signing information
- Any other attributes in the signature envelope

Examples

The following example displays software authentication related information for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting:

```
Router(mmode-prompt
)# show software authenticity running
SYSTEM IMAGE
-------------------
Image type : Development
Signer Information
Common Name : xxx
Organization Unit : xxx
Organization Name : xxx
Certificate Serial Number : xxx
Hash Algorithm : xxx
Signature Algorithm : 2048-bit RSA
Key Version : xxx
Verifier Information
Verifier Name : ROMMON 2
ROMMON 2
-------------------
Image type : Development
Signer Information
Common Name : xxx
Organization Unit : xxx
Organization Name : xxx
Certificate Serial Number : xxx
Hash Algorithm : xxx
Signature Algorithm : 2048-bit RSA
Key Version : xxx
Verifier Information
Verifier Name : ROMMON 2
```

The following table describes the significant fields shown in the display.
Table 169: show software authenticity running Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM IMAGE</td>
<td>Section of the output displaying the system image information.</td>
</tr>
<tr>
<td>Image type</td>
<td>Displays the type of image.</td>
</tr>
<tr>
<td>Common Name</td>
<td>Displays the name of the software manufacturer.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Displays the hardware the software image is deployed on.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Displays the owner of the software image.</td>
</tr>
<tr>
<td>Certificate Serial Number</td>
<td>Displays the certificate serial number for the digital signature.</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>Displays the type of hash algorithm used in digital signature verification.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Displays the type of signature algorithm used in digital signature verification.</td>
</tr>
<tr>
<td>Key Version</td>
<td>Displays the key version used for verification.</td>
</tr>
<tr>
<td>Verifier Name</td>
<td>Name of the program responsible for performing the digital signature verification.</td>
</tr>
<tr>
<td>Verifier Version</td>
<td>Version of the program responsible for performing the digital signature verification.</td>
</tr>
<tr>
<td>ROMMON 2</td>
<td>Section of the output displaying the current ROM monitor (ROMMON) information.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show software authenticity file</td>
<td>Displays the software authenticity related information for the loaded image file.</td>
</tr>
<tr>
<td>show software authenticity keys</td>
<td>Displays the software public keys that are in the storage with the key types.</td>
</tr>
</tbody>
</table>

show software package

To display information about a specific bundle or package file, use the `show software package` command in privileged EXEC mode.

```
show software package  bundle or package url [ {detail} ] [ {verbose} ]
```

Syntax Description

<table>
<thead>
<tr>
<th>bundle or package url</th>
<th>Specify the name of the bundle or package file whose information should be displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(optional) This command option is intended to provide additional details about the specified package or bundle file. Currently, no additional information is displayed.</td>
</tr>
</tbody>
</table>
The 'show software package' command displays information about the specified bundle or package file. If a package file is specified, this command displays information from its package metadata. If a bundle file is specified, this command displays information from its bundle metadata, and also information from the package metadata of each package included in the bundle.

Examples

The following example shows the `show software package` output for a bundle file.

```
infra-p2-3#show software package flash:cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
Size: 22076688
Timestamp: 2012-11-15 11:53:50 UTC
Header size: 2928 bytes

Internal package information:
  Name: rp_super
  BuildTime: Thu Nov 15 01:55:09 PST 2012
  ReleaseDate: Thu Nov 15 01:55:09 PST 2012
  RouteProcessor: mips
  Platform: ng3k
  User: udonthi
  PackageName: cat3k_caa-universalk9
  Build: 03.09.19.EMP
  Dependencies: PROVIDES:cat3k_caa-base,03.09.19.EMP,mips;cat3k_caa-infra,03.09.19.EMP,mips;cat3k_caa-platform,03.09.19.EMP,mips;cat3k_caa-iosd-universalk9,150-9.19.EMP,mips;cat3k_caa-wcm,03.09.19.EMP,mips;cat3k_caa-drivers,03.09.19.EMP,mips;
  BuildType: Production

Package is bootable from media and tftp.
Package contents:

Package: cat3k_caa-base.SSA.03.09.19.EMP.pkg
Size: 74390336
Timestamp: 2012-11-15 11:55:30 UTC
Header size: 412 bytes

Internal package information:
  Name: rp_base
  BuildTime: Thu Nov 15 01:55:09 PST 2012
  ReleaseDate: Thu Nov 15 01:55:09 PST 2012
  RouteProcessor: mips
  Platform: ng3k
  User: udonthi
  PackageName: cat3k_caa-base
```
Package is not bootable.

Package: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
Size: 2734772
Timestamp: 2012-11-15 11:55:37 UTC
Header size: 252 bytes

Internal package information:
Name: drivers
BuildTime: Thu Nov 15 01:54:53 PST 2012
ReleaseDate: Thu Nov 15 01:54:53 PST 2012
RouteProcessor: mips
Platform: ng3k
User: udonthi
PackageName: cat3k_caa-drivers
Build: 03.09.19.EMP
Dependencies: PROVIDES: ng3k-drivers,03.09.19.EMP,mips
BuildType: Production

Package is not bootable.

Package: cat3k_caa-infra.SSA.03.09.19.EMP.pkg
Size: 32465772
Header size: 436 bytes

Internal package information:
Name: rp_infra
BuildTime: Thu Nov 15 01:53:08 PST 2012
ReleaseDate: Thu Nov 15 01:53:08 PST 2012
RouteProcessor: mips
Platform: ng3k
User: udonthi
PackageName: cat3k_caa-infra
Build: 03.09.19.EMP
Dependencies: PROVIDES: nova-infra,03.09.19.EMP,mips;
nova-infralibs,03.09.19.EMP,mips;
nova-web,03.09.19.EMP,mips;
nova-shell,03.09.19.EMP,mips;
nova-console-relay,03.09.19.EMP,mips;
nova-mgmt,03.09.19.EMP,mips;
nova-ng3k-flash,03.09.19.EMP,mips
Requires: #WORKSWITH: #CONFLICTS:
BuildType: Production

Package is not bootable.

Size: 30384940
Timestamp: 2012-11-15 11:55:34 UTC
Header size: 372 bytes

Internal package information:
Name: rp_iosd
BuildTime: Thu Nov 15 01:54:09 PST 2012
ReleaseDate: Thu Nov 15 01:54:09 PST 2012
RouteProcessor: mips
Platform: ng3k
User: udonthi
PackageName: cat3k_caa-iosd-universalk9

Build: 150-9.19.EMP
Dependencies: PROVIDES: iosd-stuff,03.09.19.EMP,mips; nova-ioslibs-required, 03.09.19.EMP,mips; ioucon,150-9.19.EMP,mips;
ng3k-iosd-universalk9,150-9.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:
BuildType: Production

Package is not bootable.

Package: cat3k_caa-platform.SSA.03.09.19.EMP.pkg
Size: 18148064
Header size: 296 bytes

Internal package information:
Name: rp_platform
BuildTime: Thu Nov 15 01:53:39 PST 2012
ReleaseDate: Thu Nov 15 01:53:39 PST 2012
RouteProcessor: mips
Platform: ng3k
User: udonthi
PackageName: cat3k_caa-platform
Build: 03.09.19.EMP
Dependencies: PROVIDES: nova-platformlibs-required,03.09.19.EMP,mips;
ng3k-platform,03.09.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:
BuildType: Production

Package is not bootable.

Package: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
Size: 62638800
Timestamp: 2012-11-15 11:55:37 UTC
Header size: 280 bytes

Internal package information:
Name: rp_wcm
BuildTime: Thu Nov 15 01:54:34 PST 2012
ReleaseDate: Thu Nov 15 01:54:34 PST 2012
RouteProcessor: mips
Platform: ng3k
User: udonthi
PackageName: cat3k_caa-wcm
Build: 03.09.19.EMP
Dependencies: PROVIDES: wcm-ng3k,03.09.19.EMP,mips; nova-wcmlibs-required, 03.09.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:
BuildType: Production

Package is not bootable.

infra-p2-3#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that are no longer in use.</td>
</tr>
<tr>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
</tbody>
</table>
**Command | Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the auto-rollback command option of the software install command.</td>
</tr>
<tr>
<td>software install source switch</td>
<td>Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.</td>
</tr>
<tr>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.</td>
</tr>
<tr>
<td>show version</td>
<td>To display information about the currently loaded software along with hardware and device information, use the show version command.</td>
</tr>
</tbody>
</table>

---

**show software installer rollback-timer**

The `show software installer rollback-timer` command displays the current auto-rollback timer status for a standalone platform or all switches in a stacked system.

**show software installer rollback-timer**

**Command Default**

There are no command options.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3 SE</td>
<td>This command was integrated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

There are no command options.

**Examples**

To show the auto-rollback timer status for the current switch, perform the following.

```infra-p2-3#show software installer rollback-timer
Switch# Status Duration
-----------------------------
1   active 00:31:28
2   active 00:31:43
```

```infra-p2-3#
infra-p2-3#show software installer rollback-timer
```
Switch# | Status | Duration  
-------|--------|----------
1      | inactive | -        
2      | inactive | -        

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that are no longer in use.</td>
</tr>
<tr>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
<tr>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the auto-rollback command option of the software install command.</td>
</tr>
<tr>
<td>software install source switch</td>
<td>Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.</td>
</tr>
<tr>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.</td>
</tr>
<tr>
<td>show version</td>
<td>To display information about the currently loaded software along with hardware and device information, use the show version command.</td>
</tr>
</tbody>
</table>

show stacks

To monitor the stack usage of processes and interrupt routines, use the `show stacks` command in EXEC mode.

```
show stacks PID
```

**Syntax Description**

`PID`  Process identifier of the process that allocated the stack. The value ranges from 1 to 8192.

**Command Modes**

Privilege EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The display from this command includes the reason for the last system reboot. If the system was reloaded because of a system failure, a saved system stack trace is displayed. This information is of use only to your technical support representative in analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

Use the `show stacks PID` command to print the call stack of the process with ID ranging from 1 to 8192. This command displays the following information:

- Stack segment: Where the process stack lies in the memory.
- List of FP: `<address>`: The Frame Pointer (FP) for each frame in the call stack.
- List of RA: `<address>`: The Return Address (RA) of each frame in the call stack.

Examples

The following is a sample output from the `show stacks` command following a system failure:

```
Device# show stacks
Minimum process stacks:
Free/Size   Name
652/1000    Router Init
726/1000    Init
744/1000    BGP Open
686/1200    Virtual Exec
Interrupt level stacks:
Level   Called Free/Size   Name
1       0 1000/1000    env-flash
3       738 900/1000    Multiport Communications Interfaces
5       178 970/1000    Console UART
System was restarted by bus error at PC 0xAD1F4, address 0xD0D0D1A
GS Software (GS3), Version 9.1(0.16), BETA TEST SOFTWARE
Compiled Tue 11-Aug-92 13:27 by jthomas
Stack trace from system failure:
FP: 0x29C158, RA: 0xACFD4
FP: 0x29C184, RA: 0xAD20C
FP: 0x29C1B0, RA: 0xACFD4
FP: 0x29C1DC, RA: 0xAD304
FP: 0x29C1F8, RA: 0xAF774
FP: 0x29C214, RA: 0xAF83E
FP: 0x29C228, RA: 0x3E0CA
FP: 0x29C244, RA: 0x3BD3C
```

The following is a sample output from the `show stacks PID` command:

```
Device# show stack 10
Process 10: WATCH_AFS
  Stack segment 0x21668518 - 0x216690D0
    FP: 0x21669068, RA: 0x31A3D79C

Device# show stack 100
Process 100: dev_device_inserted
  Stack segment 0x418D1CC8 - 0x418D2880
    FP: 0x418D2830, RA: 0x30488210

Device# show stack 200
Process 200: WAAS Process
  Stack segment 0x41B76DB8 - 0x41B79C98
    FP: 0x41B79BE8, RA: 0x335ABEB4

Device# sh stack 311
Process 311: Virtual Exec
```
show startup-config

The `more nvram:startup-config` command has been replaced by the `show startup-config` command. See the description of the `more` command in the “Cisco IOS File System Commands” chapter for more information.

show subsys

To display the subsystem information, use the `show subsys` command in privileged EXEC mode.

```
show subsys [[class class]name name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>(Optional) Displays the subsystems of the specified class. Valid classes are</td>
</tr>
<tr>
<td></td>
<td>driver, ehsa, ifs, kernel, library, license, management, microcode,</td>
</tr>
<tr>
<td></td>
<td>pre-ehsa, pre-driver, protocol, registry, and sysinit.</td>
</tr>
<tr>
<td>name</td>
<td>(Optional) Displays the specified subsystem. Use the asterisk character (*) as</td>
</tr>
<tr>
<td></td>
<td>a wildcard at the end of the name to list all subsystems, starting with the</td>
</tr>
<tr>
<td></td>
<td>specified characters.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3</td>
<td>This command was modified. The <code>ehsa</code>, <code>ifs</code>, <code>microcode</code>, <code>pre-driver</code>, and</td>
</tr>
<tr>
<td></td>
<td><code>sysinit</code> classes were added.</td>
</tr>
<tr>
<td>12.3T</td>
<td>This command was modified. The <code>pre-ehsa</code> class was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was modified. The <code>driver</code>, <code>ehsa</code>, <code>kernel</code>, <code>library</code>, <code>management</code>, <code>pre-driver</code>, <code>pre-ehsa</code>, <code>protocol</code>, and <code>registry</code> classes were added.</td>
</tr>
<tr>
<td>12.2(35)SE2</td>
<td>This command was modified. The <code>driver</code>, <code>ehsa</code>, <code>kernel</code>, <code>library</code>, <code>license</code>, <code>management</code>, <code>pre-driver</code>, <code>pre-ehsa</code>, <code>protocol</code>, and <code>registry</code> classes were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show subsys` command to confirm that all required features are in the running image.

**Examples**

The following is sample output from the `show subsys` command:

```
Router# show subsys
Name    Class     Version
```
The following is sample output from the `show subsys` command that includes the `license` class:

```
Router# show subsys name license
Name          Class      Version
license_mgmt_local Management 1.000.001
license_admin_local Management 1.000.001
license_debug_core Management 1.000.001
license_test_ui Management 1.000.001
test_license_parser Management 1.000.001
license_ui Management 1.000.001
license_parser Management 1.000.001
license.registry Registry 1.000.001
license_client License 1.000.001
```

The table below describes the fields shown in the display.

**Table 170: show subsys Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the subsystem.</td>
</tr>
<tr>
<td>Class</td>
<td>Class of the subsystem. Possible classes include Driver, Ehsa, Ifs, Kernel, Library, License, Management, Microcode, Pre-Ehsa, Pre-driver, Protocol, Registry, and Sysinit.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the subsystem.</td>
</tr>
</tbody>
</table>

**show sup-bootflash**

To display information about the sup-bootflash file system, use the `show sup-bootflash` command in privileged EXEC mode.

```
show sup-bootflash [{all|chips|filesys}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Displays all possible Flash information.</td>
</tr>
</tbody>
</table>
show sup-bootflash

**chips** (Optional) Displays information about the Flash chip.

**filesys** (Optional) Displays information about the file system.

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.217dSX</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SX</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display a summary of bootflash information:

```
Router# show sup-bootflash
-#- ED --type-- --crc--- --seek-- nlen --length-- -----date/time------ name
1 .. image EBC8FC4D A7487C 6 10700796 Nov 19 1999 07:07:37 halley
2 .. unknown C7EB077D EE2620 25 4644130 Nov 19 1999 07:50:44 cat6000-sup_5-3-3-CSX.bin
645600 bytes available (15345184 bytes used)
```

Router#

This example shows how to display all bootflash information:

```
Router# show sup-bootflash all
-#- ED --type-- --crc--- --seek-- nlen --length-- -----date/time------ name
1 .. image EBC8FC4D A7487C 6 10700796 Nov 19 1999 07:07:37 halley
2 .. unknown C7EB077D EE2620 25 4644130 Nov 19 1999 07:50:44 cat6000-sup_5-3-3-CSX.bin
645600 bytes available (15345184 bytes used)
---------- FILE SYSTEM STATUS ----------
Device Number = 2
DEVICE INFO BLOCK: bootflash
  Magic Number = 6887635  File System Vers = 10000  (1.0)
  Length = 1000000  Sector Size = 40000
  Programming Algorithm = 19  Erased State = FFFFFFFF
  File System Offset = 40000  Length = F40000
  MONLIB Offset = 100  Length = F568
  Bad Sector Map Offset = 3FFF8  Length = 8
  Squeeze Log Offset = F80000  Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
Spares:
  STATUS INFO:
    Writable
    NO File Open for Write
    Complete Stats
    No Unrecovered Errors
    No Squeeze in progress
USAGE INFO:
  Bytes Used = EA2620  Bytes Available = 9D9E0
```
This example shows how to display information about the Flash chip:

Router# `show sup-bootflash chips`

----- Intel SCS Status/Register Dump -----  

COMMON MEMORY REGISTERS: Bank 0
Intelligent ID Code : 890089
Compatible Status Reg: 800080

DEVICE TYPE:
  Layout : Paired x16 Mode
  Write Queue Size : 64
  Queued Erase Supported : No

Router#

This example shows how to display information about the file system:

Router# `show sup-bootflash filesys`

-------- FILE SYSTEM STATUS --------

Device Number = 2

DEVICE INFO BLOCK: bootflash
  Magic Number = 6887635 File System Vers = 10000 (1.0)
  Length = 1000000 Sector Size = 40000
  Programming Algorithm = 19 Erased State = FFFFFFFF
  File System Offset = 40000 Length = F40000
  MONLIB Offset = 100 Length = F568
  Bad Sector Map Offset = 3FFF8 Length = 8
  Squeeze Log Offset = F80000 Length = 40000
  Squeeze Buffer Offset = FC0000 Length = 40000
  Num Spare Sectors = 0

Spares:

STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  NO Unrecovered Errors
  NO Squeeze in progress

USAGE INFO:
  Bytes Used = EA2620 Bytes Available = 9D9E0
  Bad Sectors = 0 Spared Sectors = 0
  OK Files = 2 Bytes = EA2520
  Deleted Files = 0 Bytes = 0
  Files w/Errors = 0 Bytes = 0

Router#
show system jumbomtu

To display the global maximum transmission unit (MTU) setting, use the `show system jumbomtu` command in privileged EXEC mode.

```
show system jumbomtu
```

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to display the global MTU setting:

```
Router# show system jumbomtu
Global Ethernet MTU is 1550 bytes.
Router#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system jumbomtu</td>
<td>Sets the maximum size of the Layer 2 and Layer 3 packets.</td>
</tr>
</tbody>
</table>

show tech-support

To display general information about the router when it reports a problem, use the `show tech-support` command in privileged EXEC mode.

```
show tech-support [page] [password] [{CEF|ip multicast} [vrf vrf-name]isis|mpls|ipsec [peer ipv4 address | vrf vrf-name]|ospp [process-id][detail]|rsvp|voice|wccp ]
```

Cisco 7600 Series

```
show tech-support [{CEF|ip multicast} [vrf vrf-name]isis|password [page]|platform|page|rsvp]}
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>page</td>
<td>(Optional) Causes the output to display a page of information at a time.</td>
</tr>
<tr>
<td>password</td>
<td>(Optional) Leaves passwords and other security information in the output.</td>
</tr>
<tr>
<td>cef</td>
<td>(Optional) Displays show command output specific to Cisco Express Forwarding.</td>
</tr>
<tr>
<td>ipc</td>
<td>(Optional) Displays show command output specific to Inter-Process Communication (IPC).</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ipmulticast</strong></td>
<td>(Optional) Displays <code>show</code> command output related to the IP Multicast configuration, including Protocol Independent Multicast (PIM) information, Internet Group Management Protocol (IGMP) information, and Distance Vector Multicast Routing Protocol (DVMRP) information.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Specifies a multicast Virtual Private Network (VPN) routing and forwarding instance (VRF).</td>
</tr>
<tr>
<td><strong>ipsec</strong></td>
<td>(Optional) Displays <code>show</code> command output related to the IPsec configuration.</td>
</tr>
<tr>
<td><strong>peer ipv4 address</strong></td>
<td>(Optional) Specifies the IPv4 address of a peer.</td>
</tr>
<tr>
<td><strong>isis</strong></td>
<td>(Optional) Displays <code>show</code> command output specific to Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System Protocol (IS-IS).</td>
</tr>
<tr>
<td><strong>mpls</strong></td>
<td>(Optional) Displays <code>show</code> command output specific to Multiprotocol Label Switching (MPLS) forwarding and applications.</td>
</tr>
<tr>
<td>**ospf [process-id</td>
<td>detail]**</td>
</tr>
<tr>
<td><strong>rsvp</strong></td>
<td>(Optional) Displays <code>show</code> command output specific to Resource Reservation Protocol (RSVP) networking.</td>
</tr>
<tr>
<td><strong>voice</strong></td>
<td>(Optional) Displays <code>show</code> command output specific to voice networking.</td>
</tr>
<tr>
<td><strong>wccp</strong></td>
<td>(Optional) Displays <code>show</code> command output specific to Web Cache Communication Protocol (WCCP).</td>
</tr>
<tr>
<td><strong>platform</strong></td>
<td>(Optional) Displays platform-specific <code>show</code> command output.</td>
</tr>
</tbody>
</table>

**Command Default**

The output scrolls without page breaks. Passwords and other security information are removed from the output.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(7), 11.2(16)</td>
<td>This command was modified. The output for this command was expanded to show additional information for <code>boot</code>, <code>bootflash</code>, <code>context</code>, and <code>traffic</code> for all enabled protocols.</td>
</tr>
<tr>
<td>12.0</td>
<td>This command was modified. The output for this command was expanded to show additional information for <code>boot</code>, <code>bootflash</code>, <code>context</code>, and <code>traffic</code> for all enabled protocols. The <code>cef</code>, <code>ipmulticast</code>, <code>isis</code>, <code>mpls</code>, and <code>ospf</code> keywords were added to this command.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was modified. Support for AppleTalk EIGRP, Apollo Domain, Banyan VINES, Novell Link-State Protocol, and XNS was removed from Cisco IOS software.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was modified. The output of this command was expanded to include the output from the show inventory command.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
</tbody>
</table>
| 12.2(30)S    | This command was modified. The show tech-support ipmulticast command was changed as follows:  
|              | • Support for bidirectional PIM and Multicast VPN (MVPN) was added.  
|              | • The vrf vrf-name keyword and argument were added.  

The output of the show tech-support ipmulticast command (without the vrf vrf-name keyword and argument) was changed to include the output from these commands:  
|              | • show ip pim int df  
|              | • show ip pim mdt  
|              | • show ip pim mdt bgp  
|              | • show ip pim rp metric |
| 12.3(16)     | This command was integrated into Cisco IOS Release 12.3(16). |
| 12.2(18)SXF  | This command was modified. The show tech-support ipmulticast command was changed as follows:  
|              | • Support for bidirectional PIM and MVPN was added.  
|              | • The vrf vrf-name keyword and argument were added.  

The output of the show tech-support ipmulticast vrf command was changed to include the output from these commands:  
|              | • show mls ip multicast rp-mapping gm-cache  
|              | • show mmls gc process  
|              | • show mmls msc rpdf-cache  

The output of the show tech-support ipmulticast command (without the vrf vrf-name keyword and argument) was changed to include the output from these commands:  
|              | • show ip pim int df  
|              | • show ip pim mdt  
|              | • show ip pim mdt bgp  
|              | • show ip pim rp metric  

Support to interrupt and terminate the show tech-support output was added.
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(7)</td>
<td>This command was integrated into Cisco IOS Release 12.4(7).</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(9)T</td>
<td>This command was modified. The output of this command was expanded to include partial <code>show dmvpn details</code> command output.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The <code>wccp</code> and <code>voice</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The <code>wccp</code> keyword was added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was modified. The <code>wccp</code> keyword was added.</td>
</tr>
<tr>
<td>15.3(2)T</td>
<td>This command was modified. The output was extended to include select output for the Group Domain of Interpretation (GDOI) configuration on key servers and group members.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was modified. The output was extended to include select output for the GDOI configuration on key servers and group members.</td>
</tr>
<tr>
<td>15.4(1)T</td>
<td>This command was modified. The output of the <code>ipsec</code> keyword was modified.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To interrupt and terminate the `show tech-support` output, simultaneously press and release the `CTRL`, `ALT`, and `6` keys.

Press the **Return** key to display the next line of output, or press the **Spacebar** to display the next page of information. If you do not enter the `page` keyword, the output scrolls (that is, it does not stop for page breaks).

If you do not enter the `password` keyword, passwords and other security-sensitive information in the output are replaced with the label “&lt;removed&gt;.”

The `show tech-support` command is useful for collecting a large amount of information about your routing device for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

Effective with CSCsg71173, password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP) passwords are not displayed in the output of this command.

---

**Note**

This command can generate a very large amount of output. You may want to redirect the output to a file using the `show inventory | redirect url` command syntax extension. Redirecting the output to a file also makes sending this output to your technical support representative easier. For more information about this option, see the command documentation for `show <command> | redirect`.

The `show tech-support` command displays the output of a number of `show` commands at once. The output from this command varies depending on your platform and configuration. For example, access servers display voice-related `show` command output. Additionally, the show protocol traffic commands are displayed for only the protocols enabled on your device. For a sample display of the output of the `show tech-support` command, see the individual `show` command listed.
If you enter the `show tech-support` command without arguments, the output displays, but is not limited to, the equivalent of these `show` commands:

- `show appletalk traffic`
- `show bootflash`
- `show bootvar`
- `show buffers`
- `show cdp neighbors`
- `show cef`
- `show clns traffic`
- `show context`
- `show controllers`
- `show crypto gdoi`
- `show crypto gdoi gm`
- `show crypto gdoi gm acl`
- `show crypto gdoi gm pubkey`
- `show crypto gdoi gm rekey detail`
- `show crypto gdoi gm replay`
- `show crypto gdoi ipsec sa`
- `show crypto gdoi ks`
- `show crypto gdoi ks acl`
- `show crypto gdoi ks coop`
- `show crypto gdoi ks coop version`
- `show crypto gdoi ks identifier detail`
- `show crypto gdoi ks member`
- `show crypto gdoi ks policy`
- `show crypto gdoi ks rekey`
- `show crypto gdoi ks replay`
- `show decnet traffic`
- `show disk0: all`
- `show dmvpn details`
- `show environment`
- `show fabric channel-counters`
• show file systems
• show interfaces
• show interfaces switchport
• show interfaces trunk
• show ip interface
• show ip traffic
• show logging
• show mac-address-table
• show module
• show power
• show processes cpu
• show processes memory
• show running-config
• show spanning-tree
• show stacks
• show version
• show vlan

Crypto information is not duplicated by the **show dmvpn details** command output.

---

**Note**

When the **show tech-support** command is entered on a virtual switch (VS), the output displays the output of the **show module** command and the **show power** command for both the active and standby switches.

Use of the optional **cef, ip, ipmulticast, isis, mpls, ospf, or rsvp** keywords provides a way to display a number of **show** commands specific to a particular protocol or process in addition to the show commands listed previously.

For example, if your Technical Assistance Center (TAC) support representative suspects that you have a problem in your Cisco Express Forwarding (CEF) configuration, you may be asked to provide the output of the **show tech-support cef command**. The **show tech-support [page] [password] cef** command will display the output from the following commands in addition to the output for the standard **show tech-support** command:

• show adjacency summary
• show cef drop
• show cef events
• show cef interface
• show cef not-cef-switched
• show cef timers
• show interfaces stats
• show ip cef events summary
• show ip cef inconsistency records detail
• show ip cef summary

If you enter the ipmulticast keyword, the output displays, but is not limited to, these show commands:
• show ip dvmrp route
• show ip igmp groups
• show ip igmp interface
• show ip mcache
• show ip mroute
• show ip mroute count
• show ip pim interface
• show ip pim interface count
• show ip pim interface df
• show ip pim mdt
• show ip pim mdt bgp
• show ip pim neighbor
• show ip pim rp
• show ip pim rp metric
• show mls ip multicast rp-mapping gm-cache
• show mmls ge process
• show mmls msc rpdf-cache

If you enter the wccp keyword, the output displays, but is not limited to, these show commands:
• show ip wccp  service-number
• show ip wccp interfaces cef

Examples

For a sample display of the output from the show tech-support command, refer to the documentation for the show commands listed in the “Usage Guidelines” section.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><code>show appletalk traffic</code></td>
<td>Displays statistics about AppleTalk traffic, including MAC IP traffic.</td>
<td></td>
</tr>
<tr>
<td><code>show bootflash</code></td>
<td>Displays the contents of boot flash memory.</td>
<td></td>
</tr>
<tr>
<td><code>show bootvar</code></td>
<td>Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.</td>
<td></td>
</tr>
<tr>
<td><code>show buffers</code></td>
<td>Displays statistics for the buffer pools on the network server.</td>
<td></td>
</tr>
<tr>
<td><code>show cdp neighbors</code></td>
<td>Displays detailed information about neighboring devices discovered using Cisco Discovery Protocol.</td>
<td></td>
</tr>
<tr>
<td><code>show cef</code></td>
<td>Displays information about packets forwarded by Cisco Express Forwarding.</td>
<td></td>
</tr>
<tr>
<td><code>show clns traffic</code></td>
<td>Displays a list of the CLNS packets this router has seen.</td>
<td></td>
</tr>
<tr>
<td>`show &lt; command &gt;</td>
<td>redirect`</td>
<td>Redirects the output of any <code>show</code> command to a file.</td>
</tr>
<tr>
<td><code>show context</code></td>
<td>Displays context data.</td>
<td></td>
</tr>
<tr>
<td><code>show controllers</code></td>
<td>Displays information that is specific to the hardware.</td>
<td></td>
</tr>
<tr>
<td><code>show controllers tech-support</code></td>
<td>Displays general information about a VIP card for problem reporting.</td>
<td></td>
</tr>
<tr>
<td><code>show crypto gdoi</code></td>
<td>Displays information about a GDOI configuration.</td>
<td></td>
</tr>
<tr>
<td><code>show disk:0</code></td>
<td>Displays flash or file system information for a disk located in slot 0:</td>
<td></td>
</tr>
<tr>
<td><code>show dmvpn details</code></td>
<td>Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.</td>
<td></td>
</tr>
<tr>
<td><code>show environment</code></td>
<td>Displays temperature, voltage, and blower information on the Cisco 7000 series routers, Cisco 7200 series routers, Cisco 7500 series routers, Cisco 7600 series routers, Cisco AS5300 series access servers, and the Gigabit Switch Router.</td>
<td></td>
</tr>
<tr>
<td><code>show fabric channel counters</code></td>
<td>Displays the fabric channel counters for a module.</td>
<td></td>
</tr>
<tr>
<td><code>show file system</code></td>
<td>Lists available file systems.</td>
<td></td>
</tr>
<tr>
<td><code>show interfaces</code></td>
<td>Displays statistics for all interfaces configured on the router or access server.</td>
<td></td>
</tr>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Displays the administrative and operational status of a switching (nonrouting) port.</td>
<td></td>
</tr>
<tr>
<td><code>show interfaces trunk</code></td>
<td>Displays the interface-trunk information.</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>show inventory</td>
<td>Displays the product inventory listing and UDI of all Cisco products installed in the networking device.</td>
<td></td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays the usability status of interfaces configured for IP.</td>
<td></td>
</tr>
<tr>
<td>show ip traffic</td>
<td>Displays statistics about IP traffic.</td>
<td></td>
</tr>
<tr>
<td>show ip wccp</td>
<td>Displays global statistics related to WCCP.</td>
<td></td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of syslog and the contents of the standard system logging buffer.</td>
<td></td>
</tr>
<tr>
<td>show mac-address table</td>
<td>Displays the MAC address table.</td>
<td></td>
</tr>
<tr>
<td>show module</td>
<td>Displays module status and information.</td>
<td></td>
</tr>
<tr>
<td>show power</td>
<td>Displays the current power status of system components.</td>
<td></td>
</tr>
<tr>
<td>show processes cpu</td>
<td>Displays information about the active processes.</td>
<td></td>
</tr>
<tr>
<td>show processes memory</td>
<td>Displays the amount of memory used.</td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the current configuration of your routing device.</td>
<td></td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>Displays information about the spanning tree state.</td>
<td></td>
</tr>
<tr>
<td>show stacks</td>
<td>Displays the stack usage of processes and interrupt routines.</td>
<td></td>
</tr>
<tr>
<td>show version</td>
<td>Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.</td>
<td></td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays VLAN information.</td>
<td></td>
</tr>
</tbody>
</table>

**show template**

To display template information, use the **show template** command in user EXEC or privileged EXEC mode.

```
show template [template-name]
```

**Syntax Description**

- `template-name` (Optional) The template name.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRE</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Aggregation Services Router.

### Examples

The following is sample output from the `show template` command displaying template information. The fields are self-explanatory.

```
Router# show template
Template class/type Component(s)
template1 owner ppp peer dialer
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>template</code></td>
<td>Configures a particular customer profile template.</td>
</tr>
</tbody>
</table>

### show usb controllers

To display USB host controller information, use the `show usb controllers` command in privileged EXEC mode.

```
show usb controllers [controller-number]
```

**Syntax Description**

| `controller-number` | (Optional) Displays information only for the specified controller. |

**Command Default**

Information about all controllers on the system are displayed.

**Command Modes**

Privileged EXEC

**Command History**

- **Release** | **Modification**
  - 12.3(14)T | This command was introduced.
  - 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform.

**Usage Guidelines**

Use the `show usb controllers` command to display content such as controller register specific information, current asynchronous buffer addresses, and period scheduling information. You can also use this command to verify that copy operations are occurring successfully onto a USB flash module.

**Examples**

The following example is sample output from the `show usb controllers` command:

```
Router# show usb controllers
Name:1362HCD
Controller ID:1
Controller Specific Information:
  Revision:0x11
  Control:0x80
  Command Status:0x0
```
 Hardware Interrupt Status: 0x24  
 Hardware Interrupt Enable: 0x80000040  
 Hardware Interrupt Disable: 0x80000040  
 Frame Interval: 0x27782EDF  
 Frame Remaining: 0x13C1  
 Frame Number: 0x0A4C  
 LSThreshold: 0x628  
 RhDescriptorA: 0x19000202  
 RhDescriptorB: 0x0  
 RhStatus: 0x0  
 RhPort1Status: 0x100103  
 RhPort2Status: 0x100303  
 Hardware Configuration: 0x3029  
 DMA Configuration: 0x0  
 Transfer Counter: 0x1  
 Interrupt: 0x9  
 Interrupt Enable: 0x196  
 Chip ID: 0x3630  
 Buffer Status: 0x0  
 Direct Address Length: 0x80A00  
 ATL Buffer Size: 0x600  
 ATL Buffer Port: 0x0  
 ATL Block Size: 0x100  
 ATL PTD Skip Map: 0xFFFFFFFF  
 ATL PTD Last: 0x20  
 ATL Current Active PTD: 0x0  
 ATL Threshold Count: 0x1  
 ATL Threshold Timeout: 0xFF  
 
 Int Level: 1  
 Transfer Completion Codes:  
 Success : 920  
 CRC : 0  
 Bit Stuff : 0  
 Stall : 0  
 No Response : 0  
 Overrun : 0  
 Underrun : 0  
 Other : 0  
 Buffer Overrun : 0  
 Buffer Underun : 0  
 Transfer Errors:  
 Canceled Transfers : 2  
 Control Timeout : 0  
 Transfer Failures:  
 Interrupt Transfer : 0  
 Bulk Transfer : 0  
 Isochronous Transfer : 0  
 Control Transfer: 0  
 Transfer Successes:  
 Interrupt Transfer : 0  
 Bulk Transfer : 26  
 Isochronous Transfer : 0  
 Control Transfer: 894  
 USBD Failures:  
 Enumeration Failures : 0  
 No Class Driver Found: 0  
 Power Budget Exceeded: 0  
 
 USB MSCD ZCSI Class Driver Counters:  
 Good Status Failures : 3  
 Command Fail : 0  
 Good Status Timed out: 0  
 Device not Found: 0  
 Device Never Opened : 0  
 Drive Init Fail : 0  
 Illegal App Handle : 0  
 Bad API Command : 0  
 Invalid Unit Number : 0  
 Invalid Argument: 0  
 Application Overflow : 0  
 Device in use : 0  
 Control Pipe Stall : 0  
 Malloc Error : 0  
 Device Stalled : 0  
 Bad Command Code: 0  
 Device Detached : 0  
 Unknown Error : 0  
 Invalid Logic Unit Num: 0  
 
 USB Aladdin Token Driver Counters:  
 Token Inserted : 1  
 Token Removed : 0  
 Send Insert Msg Fail : 0  
 Response Txns : 434  
 Dev Entry Add Fail : 0  
 Request Txns : 434  
 Dev Entry Remove Fail: 0  
 Request Txn Fail: 0  
 Response Txn Fail : 0  
 Command Txn Fail: 0  
 Txn Invalid Dev Handle: 0
show usb device

To display USB device information, use the `show usb device` command in privileged EXEC mode.

```
show usb device [controller-ID [device-address]]
```

**Syntax Description**

- `controller-ID` (Optional) Displays information only for the devices under the specified controller.
- `device-address` (Optional) Displays information only for the device with the specified address.

**Command Default**
Information for all devices attached to the system are displayed.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into the Cisco 7200VXR NPE-G2 platform.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `show usb device` command to display information for either a USB flash drive or a USB eToken, as appropriate.

**Examples**

The following example is sample output from the `show usb device` command:

```
Router# show usb device

Host Controller:1
Address:0x1
Device Configured:YES
Device Supported:YES
Description:DiskOnKey
Manufacturer:M-Sys
Version:2.0
Serial Number:0750D84030316868
Device Handle:0x1000000
USB Version Compliance:2.0
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x8EC
Product ID:0xit5
Max. Packet Size of Endpoint Zero:64
```
Number of Configurations: 1
Speed: Full
Selected Configuration: 1
Selected Interface: 0

Configuration:
  Number: 1
  Number of Interfaces: 1
  Description:
  Attributes: None
  Max Power: 140 mA
  Interface:
    Number: 0
    Description:
    Class Code: 8
    Subclass: 6
    Protocol: 80
    Number of Endpoints: 2
    Endpoint:
      Number: 1
      Transfer Type: BULK
      Transfer Direction: Device to Host
      Max Packet: 64
      Interval: 0
    Endpoint:
      Number: 2
      Transfer Type: BULK
      Transfer Direction: Host to Device
      Max Packet: 64
      Interval: 0

Host Controller: 1
Address: 0x11
Device Configured: YES
Device Supported: YES
Description: eToken Pro 4254
Manufacturer: AKS
Version: 1.0
Serial Number:
Device Handle: 0x1010000
USB Version Compliance: 1.0
Class Code: 0xFF
Subclass Code: 0x0
Protocol: 0x0
Vendor ID: 0x529
Product ID: 0x514
Max. Packet Size of Endpoint Zero: 8
Number of Configurations: 1
Speed: Low
Selected Configuration: 1
Selected Interface: 0

Configuration:
  Number: 1
  Number of Interfaces: 1
  Description:
  Attributes: None
  Max Power: 60 mA
  Interface:
    Number: 0
    Description:
    Class Code: 255
    Subclass: 0
    Protocol: 0
    Number of Endpoints: 0

The following table describes the significant fields shown in the display.
### Table 171: `show usb device` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device handle</td>
<td>Internal memory handle allocated to the device.</td>
</tr>
<tr>
<td>Device Class code</td>
<td>The class code supported by the device. This number is allocated by the USB-IF. If this field is reset to 0, each interface within a configuration specifies its own class information, and the various interfaces operate independently. If this field is set to a value between 1 and FEH, the device supports different class specifications on different interfaces, and the interfaces may not operate independently. This value identifies the class definition used for the aggregate interfaces. If this field is set to FFH, the device class is vendor-specific.</td>
</tr>
<tr>
<td>Device Subclass code</td>
<td>The subclass code supported by the device. This number is allocated by the USB-IF.</td>
</tr>
<tr>
<td>Device Protocol</td>
<td>The protocol supported by the device. If this field is set to 0, the device does not use class-specific protocols on a device basis. If this field is set to 0xFF, the device uses a vendor-specific protocol on a device basis.</td>
</tr>
<tr>
<td>Interface Class code</td>
<td>The class code supported by the interface. If the value is set to 0xFF, the interface class is vendor specific. All other values are allocated by the USB-IF.</td>
</tr>
<tr>
<td>Interface Subclass code</td>
<td>The subclass code supported by the interface. All values are allocated by the USB-IF.</td>
</tr>
<tr>
<td>Interface Protocol</td>
<td>The protocol code supported by the interface. If this field is set to 0, the device does not use a class-specific protocol on this interface. If this field is set to 0xFF, the device uses a vendor-specific protocol for this interface.</td>
</tr>
<tr>
<td>Max Packet</td>
<td>Maximum data packet size, in bytes.</td>
</tr>
</tbody>
</table>

### `show usb driver`

To display information about registered USB class drivers and vendor-specific drivers, use the `show usb driver` command in privileged EXEC mode.

```
show usb driver [index]
```

**Syntax Description**

`[index]` (Optional) Displays information only for drivers on the specified index.

**Command Default**

Information about all drivers is displayed.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into the Cisco 7200VXR NPE-G2 platform.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS XE Release 3.6.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.6</td>
<td>This command was integrated into Cisco IOS XE Release 3.6.</td>
</tr>
</tbody>
</table>

### Examples

The following example is sample output for the `show usb driver` command:

```
Router# show usb driver

Index: 0
Owner Mask: 0x6
Class Code: 0x0
Subclass Code: 0x0
Protocol: 0x0
Interface Class Code: 0x8
Interface Subclass Code: 0x6
Interface Protocol Code: 0x50
Product ID: 0x655BD598
Vendor ID: 0x64E90000
Attached Devices:
    Controller ID: 1, Device Address: 1
Index: 1
Owner Mask: 0x1
Class Code: 0x0
Subclass Code: 0x0
Protocol: 0x0
Interface Class Code: 0x0
Interface Subclass Code: 0x0
Interface Protocol Code: 0x0
Product ID: 0x514
Vendor ID: 0x529
Attached Devices:
    Controller ID: 1, Device Address: 17
Index: 2
Owner Mask: 0x5
Class Code: 0x9
Subclass Code: 0x6249BD58
Protocol: 0x2
Interface Class Code: 0x5DC0
Interface Subclass Code: 0x5
Interface Protocol Code: 0xFFFFFFFF
Product ID: 0x2
Vendor ID: 0x1
Attached Devices: None
Index: 3
Owner Mask: 0x10
Class Code: 0x0
Subclass Code: 0x0
Protocol: 0x0
Interface Class Code: 0x0
Interface Subclass Code: 0x0
Interface Protocol Code: 0x0
Product ID: 0x0
Vendor ID: 0x0
Attached Devices: None
```

The following table describes the significant field shown in the display.
Table 17: show usb driver Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner Mask</td>
<td>Indicates the fields that are used in enumeration comparison. The driver can own different devices on the basis of their product or vendor IDs and device or interface class, subclass, and protocol codes.</td>
</tr>
</tbody>
</table>

**show usb port**

To display USB root hub port information, use the `show usb port` command in privileged EXEC mode.

```
show usb port [port-number]
```

**Syntax Description**

| port-number | (Optional) Displays information only for a specified. If the `port-number` is not issued, information for all root ports will be displayed. |

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following sample from the `show usb port` command shows the status of the port 1 on the router:

```
Router# show usb port
Port Number:0
Status:Enabled
Connection State:Connected
Speed:Full
Power State:ON
Port Number:1
Status:Enabled
Connection State:Connected
Speed:Low
Power State:ON
```

**show usb tree**

To display information about the port state and all attached devices, use the `show usb tree` command in privileged EXEC mode.

```
show usb tree
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example is sample output from the `show usb tree` command. This output shows that both a USB flash module and a USB eToken are currently enabled.

```
Router# show usb tree
[Host Id:1, Host Type:1362HCD, Number of RH-Port:2]
<Root Port0:Power=ON Current State=Enabled>
  Port0: (DiskOnKey) Addr:0x1 VID:0x08EC PID:0x0015 Configured (0x1000000)
<Root Port1:Power=ON Current State=Enabled>
  Port1: (eToken Pro 4254) Addr:0x11 VID:0x0529 PID:0x0514 Configured (0x1010000)
```

### show usbtoken

To display information about the USB eToken (such as the eToken ID), use the `show usbtoken` command in privileged EXEC mode.

```
show usbtoken [0-9]:{allfilesystem}
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-9</td>
<td>(Optional) One of the ten available flash drives you can choose from; valid values: 0-9. If you do not specify a number, 0 is used by default.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) All configuration files stored on the eToken.</td>
</tr>
<tr>
<td>filesystem</td>
<td>(Optional) Name of a configuration file.</td>
</tr>
</tbody>
</table>

#### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into the Cisco 7200VXR NPE-G2 platform.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.6</td>
<td>This command was integrated into Cisco IOS XE Release 3.6.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show usbtoken` command to verify whether a USB eToken is inserted in the router.

### Examples

The following example is sample output from the `show usbtoken` command:

```
Router# show usbtoken0
Token ID : 43353334
Token device name : token0
Vendor name : Vendor34
Product Name : Etoken Pro
Serial number : 22273a334353
Firmware version : 4.1.3.2
```
Total memory size : 32 KB
Free memory size : 16 KB
FIPS version : Yes/No
Token state : “Active” | “User locked” | “Admin locked” | “System Error” | “Unknown”
ATR (Answer To Reset) : “3B F2 98 0 FF C1 10 31 FE 55 C8 3”

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token ID</td>
<td>Token identifier.</td>
</tr>
<tr>
<td>Token device name</td>
<td>A unique name derived by the token driver.</td>
</tr>
<tr>
<td>ATR (Answer to Reset)</td>
<td>Information replied by Smart cards when a reset command is issued.</td>
</tr>
</tbody>
</table>

**show version**

To display information about the currently loaded software along with hardware and device information, use the `show version` command in user EXEC, privileged EXEC, or diagnostic mode.

**show version**

Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers
`show version[ {switch|node} ][ {running|committed|provisioned} ]`

Cisco ASR 1000 Series Routers
`show version [ rp-slot ] [ {installed | user-interface|provisioned|running} ]`

Cisco Catalyst 4500e Series Switches running IOS XE software
`show version [ rp-slot ] [ {running} ]`

Cisco Catalyst 6500 Series Routers
`show version [ epld | slot ]`

**Syntax Description**

| switch|node | (optional) Only a single switch may be specified. Default is all switches in a stacked system. |
|running | (optional) Specifies information on the files currently running. |

`cat3850` and `ct5760`: (optional) Displays information about the active package set currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the booted bundle.

| committed | (optional) Displays information about the committed package set. If no installation operations have been performed since bootup, this output will be the same as `show version running`. If any installation operations have been performed since bootup, this output will display the set of packages that will be activated/running on the next reload. |

**Note** This command option is only applicable when running in installed mode.
**provisioned** *(optional)* Specifies information on the software files that are provisioned.

Cat3850 and C5760: *(optional)* Displays information about the provisioned package set. In most cases, the provisioned package set is the same as the committed package set. These package sets will differ if an installation was performed with the ‘auto-rollback’ option and the installed packages have not yet been committed using the 'software commit' command. This command option is only applicable when running in installed mode.

**rp-slot**
Specifies the software of the RP in a specific RP slot of a Cisco ASR 1000 Series Router. Options include:

- **r0** --the RP in RP slot 0.
- **r1** --the RP in RP slot 1.
- **rp active** --the active RP.
- **rp standby** --the standby RP.

**installed**
Specifies information on the software installed on the RP.

**user-interface**
Specifies information on the files related to the user-interface.

**epld slot** *(Optional)* Specifies the software of the EPLD slot of a Cisco Catalyst 6500 Series Router.

---

**Command Default**
No default behavior or values.

**Command Modes**
User EXEC (>) Privileged EXEC (#) Diagnostic (diag)--Cisco ASR 1000 Series Routers only

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1EC</td>
<td>This command was integrated into Cisco IOS Release 12.1EC.</td>
</tr>
<tr>
<td>12.1(1a)T1</td>
<td>This command was modified to include information about the clock card on CMTS routers.</td>
</tr>
<tr>
<td>12.3BC</td>
<td>This command was integrated into Cisco IOS Release 12.3BC.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The output format of this command was updated.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>The output format of this command was updated.</td>
</tr>
<tr>
<td>12.2(33)SCA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
This command was introduced on the Cisco ASR 1000 Series Routers, and the following enhancements were introduced:

- the command became available in diagnostic mode.
- the `rp-slot`, `installed`, `user-interface`, `provisioned`, and `running` options all became available for the first time.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Release 2.1 | This command was introduced on the Cisco ASR 1000 Series Routers, and the following enhancements were introduced:  
|                    | • the command became available in diagnostic mode.  
|                    | • the `rp-slot`, `installed`, `user-interface`, `provisioned`, and `running` options all became available for the first time.  |
| 12.2(18)SX         | Added ELPD keyword and output for the Cisco Catalyst 6500 Series Router.     |
| Cisco IOS XE Release 2.4 | The output format of this command was updated.                             |
| Cisco IOS XE Release 3.1.0.SG | This command was introduced on the Cisco Catalyst 4500e Series Switches with support for the `rp-slot` parameter and `running` command option. |
| IOS XE 3.2.0 SE    | Command introduced on the Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers with support for the `switch` keyword and `running`, `provisioned` and `committed` command options. |
| Cisco IOS XE Release 3.3 SE | This command was integrated.                                               |

**Usage Guidelines**

This command displays information about the Cisco IOS software version currently running on a routing device, the ROM Monitor and Bootflash software versions, and information about the hardware configuration, including the amount of system memory. Because this command displays both software and hardware information, the output of this command is the same as the output of the `show hardware` command. (The `show hardware` command is a command alias for the `show version` command.)

Specifically, the `show version` command provides the following information:

- **Software information**
  - Main Cisco IOS image version
  - Main Cisco IOS image capabilities (feature set)
  - Location and name of bootfile in ROM
  - Bootflash image version (depending on platform)

- **Device-specific information**
  - Device name
  - System uptime
  - System reload reason
  - Config-register setting
  - Config-register settings for after the next reload (depending on platform)

- **Hardware information**
  - Platform type
  - Processor type
  - Processor hardware revision
  - Amount of main (processor) memory installed
  - Amount I/O memory installed
  - Amount of Flash memory installed on different types (depending on platform)
• Processor board ID

The output of this command uses the following format:

Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
<software-type>

Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>, <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>, <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours,
<m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform-processor-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number>

<CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache

See the Examples section for descriptions of the fields in this output.

Cisco ASR 1000 Series Routers

Entering show version without any of the options on the Cisco ASR 1000 Series Router will generate output similar to show version on other Cisco routers.

In order to understand the show version output on Cisco ASR 1000 Series Routers, it is important to understand that the individual sub-packages run the processes on the router. Among other things, the output of this command provides information on where various individual sub-packages are stored on the router, and which processes these individual sub-packages are and are not currently running.

More specifically, the command displays each individual sub-package file on the router, the hardware where the sub-package could be running, and whether the sub-package is currently being run on that hardware.

The show version provisioned command displays only the individual sub-packages that can be provisioned, which are the RP-specific sub-packages (RP Access, RP Base, RP Control, and RP IOS) and the provisioning file. The output includes the individual sub-package file, the hardware where the sub-package could be running, and whether the sub-package is currently being run on that hardware.

The command displays only the individual sub-packages that are currently active. The output includes the individual sub-package file and the hardware where the sub-package is running.

Cisco Catalyst 4500e Series Switches

Entering show version without any of the options on a Cisco Catalyst 4500e Series Switch running IOS XE software will generate output similar to show version on other Cisco platforms. One notable difference is that the output displays the IOS XE software version instead of the IOS image version.

The IOS XE software bundle includes a set of individual packages that comprise the complete set of software that runs on the switch. The show version running command displays the list individual packages that are currently active, that is, the set of packages included in the IOS XE software bundle currently running on the Cisco Catalyst 4500e Series Switch.

Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers
Entering `show version` without any of the options on a Cisco Catalyst 3850 Series Switch or Cisco 5760 Series Wireless Controller will generate output similar to `show version` on other Cisco platforms. One notable difference is that the output displays the IOS XE software version instead of the IOS image version.

The IOS XE software bundle includes a set of individual packages that comprise the complete set of software that runs on the switch or wireless controller.

The `show version running` command displays the list of individual packages that are currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the bundle.

The `show version committed` command displays information about the switch's or wireless controller's committed package set. If no installation operations have been performed since bootup, this output will be the same as `show version running`. If any installation operations have been performed since bootup, this output will display the set of packages that will be activated/running on the next reload. This command is not applicable when running in bundle mode.

The `show version provisioned` command displays information about the provisioned package set. In most cases, the provisioned package set is the same as the committed package set. These package sets will differ if an installation was performed with the `auto-rollback` option and the installed packages have not yet been committed by use of the `software commit` command. This command is not applicable when running in bundle mode.

### Examples

#### Cisco 3660 Router

The following is sample output from the `show version` command issued on a Cisco 3660 running Cisco IOS Release 12.3(4)T:

```
Router# show version

Cisco IOS Software, 3600 Software (C3660-I-M), Version 12.3(4)T
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Thu 18-Sep-03 15:37 by ccai
ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)
ROM: C3660-1 uptime is 1 week, 3 days, 6 hours, 41 minutes
System returned to ROM by power-on
System image file is "slot0:tftpboot/c3660-i-mz.123-4.T"
Cisco 3660 (R527x) processor (revision 1.0) with 57344K/8192K bytes of memory.
Processor board ID JAB055180FF
R527x CPU at 225Mhz, Implementation 40, Rev 10.0, 2048KB L2 Cache
3660 Chassis type: ENTERPRISE
2 FastEthernet interfaces
4 Serial interfaces
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of NVRAM.
16384K bytes of processor board System flash (Read/Write)
Flash card inserted. Reading filesystem...done.
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Configuration register is 0x2102
```
Cisco 7200 Router

The following is sample output from the `show version` command issued on a Cisco 7200 router running Cisco IOS Release 12.4(4)T. This output shows the total bandwidth capacity and the bandwidth capacity that is configured on the Cisco 7200. Displaying bandwidth capacity is available in Cisco IOS Release 12.2 and later releases.

```
Router# show version
Cisco IOS Software, 7200 Software (C7200-JS-M), Version 12.4(4)T, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 27-Oct-05 05:58 by ccai
ROM: System Bootstrap, Version 12.1(20000710:044039) [nlav-121E_npeb 117], DEVEE
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(16), RELEASE SOFTWARE (fc4)
router uptime is 5 days, 18 hours, 2 minutes
System returned to ROM by reload at 02:45:12 UTC Tue Feb 14 2006
System image file is "disk0:c7200-js-mz.124-4.T"
Last reload reason: Reload Command
Cisco 7206VXR (NPE400) processor (revision A) with 491520K/32768K bytes of memo.
Processor board ID 26793934
R7000 CPU at 350MHz, Implementation 39, Rev 3.2, 256KB L2 Cache
6 slot VXR midplane, Version 2.6
Last reset from power-on

PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb0_mb1 has a total of 440 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 390 bandwidth points
This configuration is within the PCI bus capacity and is supported.
Please refer to the following document "Cisco 7200 Series Port Adaptor Hardware Configuration Guidelines" on Cisco.com <http://www.cisco.com>
for c7200 bandwidth points oversubscription and usage guidelines.
4 Ethernet interfaces
2 FastEthernet interfaces
2 ATM interfaces
125K bytes of NVRAM.
62976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
125952K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2002
```

Router#

For information about PCI buses and bandwidth calculation, go to the "Cisco 7200 Series Port Adapter Installation Requirements" chapter, of theCisco 7200 Series Port Adapter Hardware Configuration Guidelines guide.

The following table describes the significant fields shown in the display.
### Table 17: show version Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>platform --Cisco hardware device name.</td>
<td></td>
</tr>
<tr>
<td>image-id --The coded software image identifier, in the format platform-features-format (for example, “c7200-g4js-mz”.</td>
<td></td>
</tr>
<tr>
<td>software-version --The Cisco IOS software release number, in the format x.y(z), where x.y is the main release identifier, z is the maintenance release number, and A, where applicable, is the special release train identifier. For example, 12.3(4)T indicates the fourth maintenance release of the 12.3T special technology release train.</td>
<td></td>
</tr>
<tr>
<td>release-type --The description of the release type. Possible values include MAINTENANCE [for example, 12.3(3)] or INTERIM [for example, 12.3(3.2)].</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>In the full software image filename, 12.3(4)T appears as 123-4.T. In the IOS Upgrade Planner, 12.3(4)T appears as 123.4T (ED).</td>
</tr>
<tr>
<td>Tip</td>
<td>Refer to “The ABC’s of Cisco IOS Networking” (available on Cisco.com) for more information on Cisco IOS software numbering and software versions.</td>
</tr>
</tbody>
</table>

Technical Support:
http://www.cisco.com/techsupport

Copyright © date-range by Cisco Systems, Inc.

The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.

Cisco IOS software, including the source code, user-help, and documentation, is copyrighted by Cisco Systems, Inc. It is Cisco’s policy to enforce its copyrights against any third party who infringes on its copyright.

ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)
The system “bootstrap” software, stored in ROM memory.

BOOTFLASH:
The system “bootflash” software, stored in Flash memory (if applicable).

device uptime is ...
The amount of time the system has been up and running.

For example:
C3660-1 uptime is 1 week, 3 days, 6 hours, 41 minutes

Cisco IOS Software, platform Software (image-id), Version software-version, release-type
For example:
Cisco IOS Software, 7200 Software (C7200-G4JS-M), Version 12.3(4)T

Cisco IOS is a registered trademark (R) of Cisco Systems, Inc.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System returned to ROM by reload-reason at timedaydate</td>
<td>Shows the last recorded reason for a system reload, and time of last reload.</td>
</tr>
<tr>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td>System returned to ROM by reload at 20:56:53 UTC Tue Nov 4 2003</td>
<td></td>
</tr>
<tr>
<td>Last reload reason: reload-reason</td>
<td>Shows the last recorded reason for a system reload.</td>
</tr>
<tr>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td>Last reload reason: Reload command</td>
<td></td>
</tr>
<tr>
<td>Last reset from reset-reason</td>
<td>Shows the last recorded reason for a system reset. Possible reset-reason values include:</td>
</tr>
<tr>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td>Last reset from power-on</td>
<td></td>
</tr>
<tr>
<td>System image file is “file-location/file-name”</td>
<td>Displays the file location (local or remote filesystem) and the system image name.</td>
</tr>
<tr>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td>System image file is &quot;slot0:tftpboot/c3660-i-mz.123-3.9.T2&quot;</td>
<td></td>
</tr>
</tbody>
</table>

For example:

- System returned to ROM by reload at 20:56:53 UTC Tue Nov 4 2003
- Last reload reason: Reload command
- Last reset from power-on

(This field was formerly labeled as the “System restarted by” field.)
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco platform (processor-type) processor (revision processor-revision-id) with free -DRAM-memory K/ packet-memory</td>
<td>This line can be used to determine how much Dynamic RAM (DRAM) is installed on your system, in order to determine if you meet the “Min. Memory” requirement for a software image. DRAM (including SDRAM) is used for system processing memory and for packet memory.</td>
</tr>
<tr>
<td>Example--Separate DRAM and Packet Memory:</td>
<td>Two values, separated by a slash, are given for DRAM: The first value tells you how DRAM is available for system processing, and the second value tells you how much DRAM is being used for Packet memory.</td>
</tr>
<tr>
<td>Cisco RSP4 (R5000) processor with 65536K/2072K bytes of memory</td>
<td>The first value, Main Processor memory, is either:</td>
</tr>
<tr>
<td>Example--Combined DRAM and Packet Memory:</td>
<td>• The amount of DRAM available for the processor, or</td>
</tr>
<tr>
<td>Cisco 3660 (R527x) processor (revision 1.0) with 57344K/8192K bytes of memory</td>
<td>• The total amount of DRAM installed on the system.</td>
</tr>
<tr>
<td>Note</td>
<td>The second value, Packet memory, is either:</td>
</tr>
<tr>
<td></td>
<td>• The total physical input/output (I/O) memory (or “Fast memory”) installed on the router (Cisco 4000, 4500, 4700, and 7500 series), or</td>
</tr>
<tr>
<td></td>
<td>• The amount of “shared memory” used for packet buffering. In the shared memory scheme (Cisco 2500, 2600, 3600, and 7200 Series), a percentage of DRAM is used for packet buffering by the router’s network interfaces.</td>
</tr>
<tr>
<td>Separate DRAM and Packet Memory</td>
<td>The terms “I/O memory” or “iomem”; “shared memory”; “Fast memory” and “PCI memory” all refer to “Packet Memory”. Packet memory is either separate physical RAM or shared DRAM.</td>
</tr>
<tr>
<td>Combined DRAM and Packet Memory</td>
<td>Separate DRAM and Packet Memory</td>
</tr>
<tr>
<td>The 4000, 4500, 4700, and 7500 series routers have separate DRAM and Packet memory, so you only need to look at the first number to determine total DRAM. In the example to the left for the Cisco RSP4, the first value shows that the router has 65536K (65,536 kilobytes, or 64 megabytes) of DRAM. The second value, 8192K, is the Packet memory.</td>
<td></td>
</tr>
<tr>
<td>Combined DRAM and Packet Memory</td>
<td>The 2500, 2600, 3600, and 7200 series routers require a minimum amount of I/O memory to support certain interface processors.</td>
</tr>
<tr>
<td>The 1600, 2500, 2600, 3600, and 7200 series routers use a fraction of DRAM as Packet memory, so you need to add both numbers to find out the real amount of DRAM. In the example to the left for the Cisco 3660, the router has 57,344 kilobytes (KB) of free DRAM and 8,192 KB dedicated to Packet memory. Adding the two numbers together gives you 57,344K + 8,192K = 65,536K, or 64 megabytes (MB) of DRAM.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration register is **value**

For example:

Configuration register is 0x2142 (will be 0x2102 at next reload)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For more details on memory requirements, see the document &quot;How to Choose a Cisco IOS® Software Release&quot; on Cisco.com.</td>
<td>Shows the current configured hex value of the software configuration register. If the value has been changed with the <code>config-register</code> command, the register value that will be used at the next reload is displayed in parenthesis. The boot field (final digit) of the software configuration register dictates what the system will do after a reset. For example, when the boot field of the software configuration register is set to 00 (for example, 0x0), and you press the NMI button on a Performance Route Processor (PRP), the user-interface remains at the ROM monitor prompt (rommon&gt;) and waits for a user command to boot the system manually. But if the boot field is set to 01 (for example, 0x1), the system automatically boots the first Cisco IOS image found in the onboard Flash memory SIMM on the PRP. The factory-default setting for the configuration register is 0x2102. This value indicates that the router will attempt to load a Cisco IOS software image from Flash memory and load the startup configuration file.</td>
</tr>
</tbody>
</table>

---

### Catalyst 6500 Series Switches and Cisco 7600 Series Routers

This example shows how to display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1 (nightly.E020626) NIG HTLY BUILD
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 26-Jun-02 06:20 by
Image text-base: 0x40008BF0, data-base: 0x419BA000
ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)
Router uptime is 2 weeks, 8 hours, 48 minutes
Time since Router switched to active is 1 minute
System returned to ROM by power-on (SP by power-on)
System image file is "sup-bootflash:c6sup22-jsv-mz"
cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.
Processor board ID SAD06210067
R7000 CPU at 300MHz, Implementation 39, Rev 3.3, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
3 Virtual Ethernet/IEEE 802.3 interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.
16384K bytes of Flash internal SIMM (Sector size 512K).
```
Configuration register is 0x2102

Router#

The following table describes the fields that are shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(nightly.E020626) NIGHTLY BUILD</td>
<td>Version number. Always specify the complete version number when reporting a possible software problem. In the example output, the version number is 12.1.</td>
</tr>
<tr>
<td>ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)</td>
<td>Bootstrap version string.</td>
</tr>
<tr>
<td>Router uptime is</td>
<td>Amount of time that the system has been up and running.</td>
</tr>
<tr>
<td>Time since Router switched to active</td>
<td>Amount of time since switchover occurred.</td>
</tr>
<tr>
<td>System restarted by</td>
<td>Log of how the system was last booted, both as a result of normal system startup and of system error. For example, information can be displayed to indicate a bus error that is typically the result of an attempt to access a nonexistent address, as follows: System restarted by bus error at PC 0xC4CA, address 0x210C0C0</td>
</tr>
<tr>
<td>System image file is</td>
<td>If the software was booted over the network, the Internet address of the boot host is shown. If the software was loaded from onboard ROM, this line reads “running default software.”</td>
</tr>
<tr>
<td>cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.</td>
<td>Remaining output in each display that shows the hardware configuration and any nonstandard software options.</td>
</tr>
<tr>
<td>Configuration register is</td>
<td>Configuration register contents that are displayed in hexadecimal notation.</td>
</tr>
</tbody>
</table>

The output of the `show version` EXEC command can provide certain messages, such as bus error messages. If such error messages appear, report the complete text of this message to your technical support specialist.

This example shows how to display the ELPD version information of a slot:

Router# `show version epld 4`

Module 4 EPLD’s:
Number of EPLD’s: 6
EPLD A : 0x5
EPLD B : 0x2
EPLD C : 0x1
EPLD D : 0x1
Cisco uBR7246VXR Router

The following is sample output from the `show version` command for a Cisco uBR7246 VXR with the cable clock card installed:

```plaintext
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-P-M), Version 12.1(10)EC, RELEASE SOFTWARE
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 02-Feb-00 16:49 by ccai
Image text-base:0x60008900, data-base:0x61192000
ROM: System Bootstrap, Version 12.0(15)SC, RELEASE SOFTWARE
VXR1 uptime is 2 days, 1 hour, 24 minutes
System returned to ROM by power-on at 10:54:38 PST Sat Feb 5 2000
System restarted at 11:01:08 PST Sat Feb 5 2000
System image file is "slot1:ubr7200-p-mz.121-0.8.T"
cisco uBR7246VXR (NPE300) processor (revision B) with 122880K/40960K bytes of memory.
Processor board ID SAB0329005N
R7000 CPU at 262Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0
Last reset from power-on
X.25 software, Version 3.0.0.
National clock card with T1 controller
1 FastEthernet/IEEE 802.3 interface(s)
2 Cable Modem network interface(s)
125K bytes of non-volatile configuration memory.
16384K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
```

The following table describes significant fields shown in these displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS (tm) 7200 Software (UBR7200-P-M), Version xx.x</td>
<td>Always specify the complete version number when reporting a possible software problem. In the example, the version number is Cisco IOS Release 12.1(10)EC.</td>
</tr>
<tr>
<td>ROM: System Bootstrap</td>
<td>Bootstrap version string.</td>
</tr>
<tr>
<td>Router uptime is</td>
<td>The amount of time the system has been up and running.</td>
</tr>
<tr>
<td>System restarted at</td>
<td>Also displayed is a log of how the system was last booted, as a result of normal system startup or system error.</td>
</tr>
<tr>
<td>System image file is</td>
<td>If the software was booted over the network, the Internet address of the boot host is shown. If the software was loaded from onboard ROM, this line reads “running default software.”</td>
</tr>
</tbody>
</table>
The remaining output in each display shows the hardware configuration and any nonstandard software options.

Configuration register is

The configuration register contents, displayed in hexadecimal notation.

The output of the `show version` command can also provide certain messages, such as bus error messages. If such error messages appear, report the complete text of this message to your technical support specialist.

**Cisco uBR10012 Router**

The following example shows sample output from the `show version` command on a Cisco uBR10012 universal broadband router running Cisco IOS Release 12.3(17b)BC4:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (UBR10K2-K9P6U2-M), Version 12.3(17b)BC4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Wed 22-Nov-06 11:41 by tinhuang
Image text-base: 0x60010F0C, data-base: 0x62480000
ROM: System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios-rommon 1 12], DEVELOPMENT SOFTWARE
ubr10k uptime is 2 days, 22 hours, 13 minutes
System returned to ROM by reload at 01:34:58 UTC Sun Jun 8 2008
System image file is "disk0:ubr10k2-k9p6u2-mz.123-17b.BC4"
Last reload reason: Reload command
This product contains cryptographic features and is subject to United States and local country laws governing import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
cisco uBR10000 (PRE2-RP) processor with 946175K/98304K bytes of memory.
Processor board ID TBA05380380
R7000 CPU at 500MHz, Implementation 39, Rev 4.1, 256KB L2, 8192KB L3 Cache
Backplane version 1.1, 8 slot
Last reset from register reset
PXF processor tmc0 is running.
PXF processor tmc1 is running.
PXF processor tmc2 is running.
PXF processor tmc3 is running.
1 TCCplus card(s)
1 FastEthernet/IEEE 802.3 interface(s)
3 Gigabit Ethernet/IEEE 802.3 interface(s)
24 Cable Modem network interface(s)
2045K bytes of non-volatile configuration memory.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
125440K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
65536K bytes of Flash internal SIMM (Sector size 512KB).
```
Secondary is up.
Secondary has 104480K bytes of memory.
Configuration register is 0x2102

Cisco ASR 1000 Series Routers

In Cisco IOS XE Release 2.4

In the following example, the show version command is responsible for displaying the packages installed, provisioned and running on the current RP.

In the following example, the command is entered on a Cisco ASR 1000 Series Router in diagnostic mode. Note that the output shows what every file that can be found in the consolidated package is or is not currently running (provisioning file, RP Access, RP Base, RP Control, RP IOS, ESP Base, SIP Base, SIP SPA).

PE23_ASR-1006#
Package: Provisioning File, version: n/a, status: active
  File: consolidated:packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: b6cb06b1ed02e041d48644340aa07783ccff2076
Package: rpbase, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpbase.02.04.00.122-33.XND.pkg, on: RP0
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: 093f2c935b9d4ed136623bc43488c6517b9a4ae
Package: rpcontrol, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP0/0
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP0/0
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpaccess.02.04.00.122-33.XND.pkg, on: RP0/0
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: 0b0d108cd268357077866897b7ffca2451b78b3
Package: rpcontrol, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP0/1
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP0/1
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpaccess.02.04.00.122-33.XND.pkg, on: RP0/1
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: 0b0d108cd268357077866897b7ffca2451b78b3
Package: rpbase, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpbase.02.04.00.122-33.XND.pkg, on: RP1
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: 093f2c935b9d4ed136623bc43488c6517b9a4ae
Package: rpcontrol, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP1/0
  Built: 2009-06-29 23:07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP1/0
  Built: 2009-06-29 23:07, by: mcpre
show protocols through showmon

show version

File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 0b0d108cd2683570778668697b7ffca2451b78b3
Package: rpcontrol, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: d71e05c824cb889048b3353257bd1619eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 0b0d108cd2683570778668697b7ffca2451b78b3
Package: espbase, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 3ae9255c7272a30f5dae319dec109ac29d9ae87
Package: espbase, version: 02.04.00.122-33.XND, status: inactive
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 3ae9255c7272a30f5dae319dec109ac29d9ae87
Package: sipbase, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: fc6e41d7de2d4e3a116b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipbase, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: fc6e41d7de2d4e3a116b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: fc6e41d7de2d4e3a116b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
Built: 2009-06-29_23.07, by: mcpre
File SHA1 checksum: fc6e41d7de2d4e3a116b6dc7e5e3a1151b788d254
Table 177: show version installed, provisioned, and running Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package:</td>
<td>The individual sub-package name.</td>
</tr>
<tr>
<td>version:</td>
<td>The consolidated package version of the individual sub-package.</td>
</tr>
<tr>
<td>status:</td>
<td>Reveals if the sub-package is active or inactive for the specific hardware component only.</td>
</tr>
<tr>
<td>File:</td>
<td>The location and filename of the individual sub-package file.</td>
</tr>
<tr>
<td>on:</td>
<td>The hardware component.</td>
</tr>
<tr>
<td>Built:</td>
<td>The date the individual sub-package was built.</td>
</tr>
<tr>
<td>File SHA1 checksum:</td>
<td>The SHA1 sum for the file. This sum can be compared against a SHA1 sum generating tool.</td>
</tr>
</tbody>
</table>

Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers

The following is sample output from the show version command on a Cisco Catalyst 3850 Series Switch that is the active switch in a 2-member stack:

infra-p2-3#show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 03.09.19.EMP EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSG5_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 15-Nov-12 01:45 by udonthi
ROM: IOS-XE ROMMON
BOOTLDR: C3850 Boot Loader (C3850-HBOOT-M) Version 1.2, engineering software (D)
infra-p2-3 uptime is 5 minutes
Uptime for this control processor is 7 minutes
System returned to ROM by reload
System image file is "flash:packages.conf"
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

License Level: Ipservices
License Type: Permanent
Next reload license Level: Ipservices

Cisco WS-C3850X-24P-PROTO2 (MIPS) processor with 2097152K bytes of physical memory.
Processor board ID FHH1515P03Y
1 Virtual Ethernet interface
56 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
160618K bytes of Crash Files at crashinfo:.
160618K bytes of Crash Files at crashinfo-1:.
706860K bytes of Flash at flash:.
698827K bytes of Flash at flash-1:.
3915670K bytes of USB Flash at usbflash0:.
OK bytes of Dummy USB Flash at usbflash0-1:.
OK bytes of at webui:.

Base Ethernet MAC Address : 64:00:f1:25:11:00
Motherboard Assembly Number : 73-12240-03
Motherboard Serial Number : FHH15130010
Model Revision Number : 01
Motherboard Revision Number : 02
Model Number : WS-C3850X-24P-PROTO2
System Serial Number : FHH1515P03Y

Switch Ports Model SW Version SW Image Mode
----- ----- ----- ---------- ---------- ----
1 32 WS-C3850X-24P-PROT 03.09.19.EMP cat3k_caa-universalk9 INSTALL
2 32 WS-C3850X-24P-PROT 03.09.19.EMP cat3k_caa-universalk9 INSTALL

Switch 01
---------
Switch uptime : 7 minutes
Base Ethernet MAC Address : 64:00:f1:25:1a:00
Motherboard Assembly Number : 73-12240-03
Motherboard Serial Number : FHH1513000T
Model Revision Number : 01
Motherboard Revision Number : 02
Model Number : WS-C3850X-24P-PROTO2
System Serial Number : FHH1515P047
Configuration register is 0x2 (will be 0x102 at next reload)

infra-p2-3# show version running
Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi

Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi

In the following example, the show version provisioned and show version committed commands are entered on a Cisco Catalyst 3850 Series Switch that is the active switch in a 2-member stack. The show version committed commands displays information about the packages in the committed package set that will be running on the next reload. The show version provisioned command displays information about the packages in the provisioned package set.
In most cases, the show version provisioned and show version committed output will display the same information, since the provisioned and committed packages sets include the same packages. The provisioned package set may differ from the committed package set in cases where a software install operation was performed with the auto-rollback command option, and the software commit command has not yet been entered. This is the case in the sample output below, where the packages from the 03.09.19.EMP were installed with the auto-rollback command option, but the 'software commit' command has not yet been entered.

The show version provisioned and show version committed commands are not applicable when the switch is booted in bundle mode.

```
infra-p2-3#show version provisioned
Package: Provisioning File, version: n/a, status: active
    File: packages.conf, on: Switch1
    Built: n/a, by: n/a

Package: Base, version: 03.09.19.EMP, status: active
    File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
    Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
    File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
    Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
    File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
    Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

    File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch1
    Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
    File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
    Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
    File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
    Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Provisioning File, version: n/a, status: active
    File: packages.conf, on: Switch2
    Built: n/a, by: n/a

Package: Base, version: 03.09.19.EMP, status: active
    File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch2
    Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
    File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch2
    Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
    File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch2
    Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

    Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
    File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch2
```
infra-p2-3#show version committed

Package: Provisioning File, version: n/a, status: active
File: packages.conf, on: Switch1
Built: n/a, by: n/a

Package: Base, version: 03.09.17.EMP, status: active
File: cat3k_caa-base.SSA.03.09.17.EMP.pkg, on: Switch1
Built: Mon Nov 12 20:27:51 PST 2012, by: udonthi

Package: Infra, version: 03.09.17.EMP, status: active
File: cat3k_caa-infra.SSA.03.09.17.EMP.pkg, on: Switch1

Package: Platform, version: 03.09.17.EMP, status: active
File: cat3k_caa-platform.SSA.03.09.17.EMP.pkg, on: Switch1
Built: Mon Nov 12 20:29:33 PST 2012, by: udonthi

Package: IOS, version: 150-9.17.EMP, status: active
File: cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg, on: Switch1
Built: Mon Nov 12 20:29:58 PST 2012, by: udonthi

Package: WCM, version: 03.09.17.EMP, status: active
File: cat3k_caa-wcm.SSA.03.09.17.EMP.pkg, on: Switch1
Built: Mon Nov 12 20:30:29 PST 2012, by: udonthi

Package: Drivers, version: 03.09.17.EMP, status: active
File: cat3k_caa-drivers.SSA.03.09.17.EMP.pkg, on: Switch1
Built: Mon Nov 12 20:31:01 PST 2012, by: udonthi
Table 178: Table 5, Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers show version running Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>The individual sub-package name.</td>
</tr>
<tr>
<td>version</td>
<td>The individual sub-package version.</td>
</tr>
<tr>
<td>status</td>
<td>Reveals if the package is active or inactive for the specific Supervisor module.</td>
</tr>
<tr>
<td>File</td>
<td>The filename of the individual package file.</td>
</tr>
<tr>
<td>on</td>
<td>The slot number of the Active or Standby Supervisor that this package is running on.</td>
</tr>
<tr>
<td>Built</td>
<td>The date the individual package was built.</td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500e Series Switches

The following is sample output from the show version command on a Cisco Catalyst 4500e Series Switch running IOS XE software:

Switch#show version
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software (cat4500e-UNIVERSALK9-M), Experimental Version 3.1.0.SG
[/nobackup/xxxx/cwab/build/arch_ppc/buildtree-ios/vob/ios/sys 100] Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 19-Apr-10 09:19 by xxxx
Cisco IOS-XE software, Copyright (c) 2005-2010 by cisco Systems, Inc.

All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License (“GPL”) Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

Image text-base: 0x100D9954, data-base: 0x14B379D8
ROM: 12.2(54r)XO(0.246)
Jawa Revision 7, Snowtrooper Revision 0x0.0x14
gsgaw-g9-35 uptime is 4 minutes
Uptime for this control processor is 5 minutes System returned to ROM by reload System image file is "tftp://1.2.3.4/tftpboot/xxxx/x.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrq.html

If you require further assistance please contact us by sending email to export@cisco.com.

License Information for 'iosd'
License Level: entservices Type: Evaluation
Next reboot license Level: entservices

cisco WS-C4510R-E (MPC8572) processor (revision 2) with 786516K/16384K bytes of memory.
Processor board ID SPE1046002Q
MPC8572 CPU at 1.5GHz, Supervisor 7
Last reset from Reload
1 Virtual Ethernet interface
84 Gigabit Ethernet interfaces
14 Ten Gigabit Ethernet interfaces

Configuration register is 0x920

Switch#

In the following example, the show version running command is entered on a Cisco Catalyst 4500e Series Switch to view the list of packages contained in the IOS XE software bundle currently loaded on the system.

Switch# show version running

Package: Base, version: 3.0.0, status: active 30
File: cat4500e-base.SSA.3.0.0.pkg, on: Slot5
From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
Built: Mon Apr 19 10:08:38 PDT 2010, by: xxxx

Package: Infra, version: 3.0.0, status: active
File: cat4500e-infra.SSA.3.0.0.pkg, on: Slot5
From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
Built: Mon Apr 19 10:09:30 PDT 2010, by: xxxx

Package: IOS, version: 150-1.XO, status: active
File: cat4500e-universalk9.SSA.150-1.XO.pkg, on: Slot5
From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
Built: Mon Apr 19 10:10:02 PDT 2010, by: xxxx

Package: Base, version: 3.0.0, status: active
File: cat4500e-base.SSA.3.0.0.pkg, on: Slot6
From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
Built: Mon Apr 19 10:08:38 PDT 2010, by: xxxx

Package: Infra, version: 3.0.0, status: active
File: cat4500e-infra.SSA.3.0.0.pkg, on: Slot6
From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
Built: Mon Apr 19 10:09:30 PDT 2010, by: xxxx

Package: IOS, version: 150-1.XO, status: active
File: cat4500e-universalk9.SSA.150-1.XO.pkg, on: Slot6
From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
Built: Mon Apr 19 10:10:02 PDT 2010, by: xxxx

Switch#
Table 179: Table 6, Cisco Catalyst 4500e Series Switches show version running Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package:</td>
<td>The individual sub-package name.</td>
</tr>
<tr>
<td>version:</td>
<td>The individual sub-package version.</td>
</tr>
<tr>
<td>status:</td>
<td>Reveals if the package is active or inactive for the specific Supervisor module.</td>
</tr>
<tr>
<td>File:</td>
<td>The filename of the individual package file.</td>
</tr>
<tr>
<td>on:</td>
<td>The slot number of the Active or Standby Supervisor that this package is running on.</td>
</tr>
<tr>
<td>From Bundle:</td>
<td>The name of the IOS XE software bundle that includes this package.</td>
</tr>
<tr>
<td>Built:</td>
<td>The date the individual package was built.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diag</td>
<td>Displays hardware and diagnostic information for a networking device, a line card, a processor, a jacket card, a chassis, or a network module.</td>
</tr>
<tr>
<td>show inventory</td>
<td>Displays the Cisco Unique Device Identifier information, including the Product ID, the Version ID, and the Serial Number, for the hardware device and hardware components.</td>
</tr>
</tbody>
</table>

show warm-reboot

To display the statistics for attempted warm reboots, use the show warm-reboot command in privileged EXEC mode.

show warm-reboot

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the show warm-reboot command to see if warm rebooting is enabled, and, if so, how many warm reloads have occurred and how much space in kilobytes (KB) is consumed by warm-reboot storage, which is the RAM area used to store the data segment that enables warm reloading to function.
Examples

The following example is sample output from the `show warm-reboot` command:

```
Router# show warm-reboot
Warm Reboot is enabled
Statistics:
10 warm reboots have taken place since the last cold reboot
XXX KB taken up by warm reboot storage
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>warm-reboot</code></td>
<td>Enables a router to warm-reboot.</td>
</tr>
</tbody>
</table>

**show wiretap**

To display the intercept status, use the `show wiretap` command in privileged EXEC mode.

```
show wiretap [{id  stream-id}idbs]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>id</code></td>
<td>(Optional) CCC ID number. The CCC ID value range is from 1 to 2147483647.</td>
</tr>
<tr>
<td><code>stream-id</code></td>
<td>(Optional) The ID value range is from 1 to 2147483647.</td>
</tr>
<tr>
<td><code>idbs</code></td>
<td>(Optional) Displays the Interface Descriptive Block (IDB) to which the Access Control List (ACL) is applied.</td>
</tr>
</tbody>
</table>

**Command Default**

If the id is not specified, information for all wiretap configurations and IDBs is displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2 (33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show wiretap` command to display the intercept status.

**Examples**

The following is sample output from the `show wiretap` command. The field descriptions are self-explanatory.

```
Router# show wiretap
Mediation Device 0x00000001
TTL = 3130
Time left = 3127 minutes
MD IP Address = 6.6.6.12
MD SNMP IF index = 0
```
show whoami

To display information about the terminal line of the current user, including host name, line number, line speed, and location, use the `show whoami` command in EXEC mode.

```
show whoami [text]
```

**Syntax Description**

```
text  (Optional) Additional data to print to the screen.
```

**Command Modes**

```
EXEC
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If text is included as an argument in the command, that text is displayed as part of the additional data about the line.

To prevent the information from being lost if the menu display clears the screen, this command always displays a `--More--` prompt before returning. Press the space bar to return to the prompt.

**Examples**

The following example is sample output from the `show whoami` command:

```
Router> show whoami
Comm Server "Router", Line 0 at 0bps. Location "Second floor, West"
--More--
Router>
```
showmon

To show both the ReadOnly and the Upgrade ROMmon image versions when you are in ROMmon mode, as well as which ROMmon image is running on the Cisco 7200 VXR or Cisco 7301 router, use the showmon command in ROM monitor mode.

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
ROM monitor mode

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(28)S</td>
<td>This command was introduced on the Cisco 7200 VXR router. It was introduced in ROMmon version 12.3(4r)T1 for the Cisco 7200 VXR router.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router. It was introduced in ROMmon version 12.3(4r)T2 for the Cisco 7301 router.</td>
</tr>
<tr>
<td>12.3(9)</td>
<td>This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use the showmon command when you are in ROM monitor mode. Use the show rom-monitor command when you are in Cisco IOS.

Examples
The following example, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, uses the showmon command in ROMmon to display both ROMmon images and to verify that the Upgrade ROMmon image is running:

rommon 1 > showmon
ReadOnly ROMMON version is:
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by Cisco Systems, Inc.
Upgrade ROMMON version is:
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by Cisco Systems, Inc.
Upgrade ROMMON currently running
Upgrade ROMMON is selected for next boot
rommon 2 >

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rommon-pref</td>
<td>Selects a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR or Cisco 7301 when you are in ROMmon.</td>
</tr>
</tbody>
</table>
showmon
slave auto-sync config through terminal-type

- slave auto-sync config through terminal-type, on page 980
slave auto-sync config through terminal-type

slave auto-sync config

To turn on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for High System Availability (HSA) using Dual RSP Cards, use the **slave auto-sync config** global configuration command. To turn off automatic synchronization, use the **no** form of the command.

```
slave auto-sync config
no slave auto-sync config
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Enabled

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command for a Cisco 7507 or Cisco 7513 router that is configured for dual RSP cards. On the Cisco 7507 and Cisco 7513 router, you can install two RSP cards in a single router to improve system availability. Dual RSP Cards is a High System Availability (HSA) feature.

In automatic synchronization mode, when you issue a **copy** EXEC command that specifies the master’s startup configuration (**nvram:startup-config**) as the target, the master also copies the same file to the slave’s startup configuration (**slavenvram:startup-config**). Use this command when implementing HSA for simple hardware backup or for software error protection to ensure that the master and slave RSP contain the same configuration files.

**Examples**
The following example turns on automatic configuration file synchronization. When the **copy system:running-config nvram:startup-config** command is entered, the running configuration is saved to the startup configurations of both the master RSP and the slave RSP.

```
Router(config)# slave auto-sync config
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller cbus</td>
<td>Displays detailed information on the cards connected to the CBus controller.</td>
</tr>
<tr>
<td>show stacks</td>
<td>Displays the stack trace and version information of the master and slave RSP cards.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the software version running on the master and slave RSP cards.</td>
</tr>
</tbody>
</table>
### slave default-slot

To specify the default slave Route Switch Processor (RSP) card on a Cisco 7507 or Cisco 7513 router, use the `slave default-slot` global configuration command.

```
slave default-slot processor-slot-number
```

**Syntax Description**

- `processor-slot-number`: Number of a processor slot that contains the default slave RSP. On the Cisco 7507 router, valid values are 2 or 3. On the Cisco 7513 router, valid values are 6 or 7. The default is the higher number processor slot.

**Command Default**

The default slave is the RSP card located in the higher number processor slot. On the Cisco 7507 router, processor slot 3 contains the default slave RSP. On the Cisco 7513 router, processor slot 7 contains the default slave RSP.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Cards. On the Cisco 7507 and Cisco 7513 router, you can install two RSP cards in a single router to improve system availability. Dual RSP Cards is a High System Availability (HSA) feature.

The router uses the default slave information when booting as follows:

- If a system boot is due to powering up the router or using the `reload` EXEC command, then the specified default slave will be the slave RSP.
- If a system boot is due to a system crash or hardware failure, then the system ignores the default slave designation, and makes the crashed or faulty RSP card the slave RSP.

**Examples**

In the following example, the user sets the default slave RSP to processor slot 2 on a Cisco 7507 router:

```
c7507(config)# slave default-slot 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reloads the operating system.</td>
</tr>
</tbody>
</table>
### slave image

To specify the image that the slave Route Switch Processor (RSP) runs on a Cisco 7507 or Cisco 7513 router, use the `slave image` command in global configuration mode.

`slave image` {system|file-url}

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>system</strong></td>
<td>Loads the slave image that is bundled with the master system image. This is the default.</td>
</tr>
<tr>
<td><strong>file-url</strong></td>
<td>The specified file in Flash file system from which the slave image will be load. If you do not specify a filename, the first file in the specified Flash file system is the default file.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is to load the image from the system bundle.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Cards. On the Cisco 7507 and Cisco 7513 router, you can install two RSP cards in a single router to improve system availability. Dual RSP Cards is a High System Availability (HSA) feature.

Use the `slave image` command to override the slave image that is bundled with the master image.

When using HSA for simple hardware backup, ensure that the slave image is in the same location on the master and the slave RSP card. Thus, if the slave RSP card becomes the master, it will be able to find the slave image and download it to the new slave.

**Note**

The default length of the bootstrap filename is 64 characters. Depending on the platform a longer bootstrap filename can be used and supported.

**Examples**

In the following example, the slave RSP is specified to run the `rsp-dw-mz.ucode.111-3.2` image from slot 0:

```
Router(config)# slave image slot0:rsp-dw-mz.ucode.111-3.2
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controller cbus</code></td>
<td>Displays detailed information on the cards connected to the CBus controller.</td>
</tr>
<tr>
<td><code>show stack s</code></td>
<td>Displays the stack trace and version information of the master and slave RSP cards.</td>
</tr>
<tr>
<td><code>show version</code></td>
<td>Displays the software version running on the master and slave RSP cards.</td>
</tr>
<tr>
<td><code>slave reload</code></td>
<td>Forces a reload of the image that the slave RSP card is running on a Cisco 7507 or Cisco 7513 router.</td>
</tr>
</tbody>
</table>

**slave reload**

To force a reload of the image that the slave Route Switch Processor (RSP) card is running on a Cisco 7507 or Cisco 7513 router, use the `slave reload` global configuration command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.2913T</td>
<td>This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may appear in 12.2S-family releases.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Cards. On the Cisco 7507 and Cisco 7513 router, you can install two RSP cards in a single router to improve system availability. Dual RSP Cards is a High System Availability (HSA) feature.

After using the `slave image` global configuration command to specify the image that the slave RSP runs on a Cisco 7507 or Cisco 7513 router, use the `slave reload` command to reload the slave with the new image. The `slave reload` command can also be used to force the slave to reboot its existing image.

**Examples**

In the following example, an inactive slave RSP card is reloaded. If the slave reloads, it will return to an active slave state. If the master RSP fails, the slave RSP will become the master.

```
c7507(config)# slave reload
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controller cbus</code></td>
<td>Displays detailed information on the cards connected to the CBus controller.</td>
</tr>
</tbody>
</table>
slave sync config

To manually synchronize configuration files on the master and slave Route Switch Processor (RSP) cards of a Cisco 7507 or Cisco 7513 router, use the `slave sync config` privileged EXEC command.

**slave sync config**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Automatic synchronization is turned on.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may appear in 12.2S-family releases.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Cards. On the Cisco 7507 and Cisco 7513 router, you can install two RSP cards in a single router to improve system availability. Dual RSP Cards is a High System Availability (HSA) feature.

This command allows you to synchronize the configuration files of the master and slave RSP cards on a case-by-case basis when you do not have automatic synchronization turned on. This command copies the master’s configuration file to the slave RSP card.

**Note**

You must use this command when you insert a new slave RSP card into a Cisco 7507 or Cisco 7513 router for the first time to ensure that the new slave is configured consistently with the master.

**Examples**

In the following example, the configuration files on the master and slave RSP card are synchronized:

c7507(config)# slave sync config
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller cbus</td>
<td>Displays detailed information on the cards connected to the CBus controller.</td>
</tr>
<tr>
<td>show stack s</td>
<td>Displays the stack trace and version information of the master and slave RSP cards.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the software version running on the master and slave RSP cards.</td>
</tr>
<tr>
<td>slave auto-sync config</td>
<td>Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for HSA.</td>
</tr>
</tbody>
</table>

slave terminal

To enable access to the slave Route Switch Processor (RSP) console, use the `slave terminal` global configuration command. To disable access to the slave RSP console, use the `no` form of this command.

```
slave terminal
no slave terminal
```

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may appear in 12.2S-family releases.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The slave console does not have enable password protection. Thus, an individual connected to the slave console port can enter privileged EXEC mode and view or erase the configuration of the router. Use the `no slave terminal` command to disable slave console access and prevent security problems. When the slave console is disabled, users cannot enter commands.

If slave console access is disabled, the following message appears periodically on the slave console:

```
%%Slave terminal access is disabled. Use "slave terminal" command in master RSP configuration mode to enable it.
```

Examples

In the following example, the user disables console access to the slave RSP:

```
c7507(config)# no slave terminal
```
## software clean

To remove any and all packages and provisioning files that are no longer in use, use the `software clean` command in Privileged EXEC mode. This command does not have a `no` form.

`software clean[ file file-url ] [ force ] [ switch nodes ] [ verbose ]`

### Syntax Description

- **file file-url**: Full path to wildcarded filename(s). Optional when running in installed mode. When no command options are specified, all unused package, bundle and provisioning files in the current boot directory will be cleaned.
- **force**: (optional) Proceeds to clean files without a prompt.
- **switch nodes**: (optional) Specifies which switch(es) should perform the clean operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
- **verbose**: (optional) Provides some additional info in the log files.

### Command Default

No software package(s) will be cleaned by default.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was integrated.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(2)E</td>
<td>This command was modified. The <code>force</code> keyword was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If no specific file to be deleted is indicated, the installer will search for unused packages and provisioning files on a given media device (e.g., `bootflash:`, `usb0:` etc) to delete. One or more nodes may be given.

With no options specified for `software clean`, all unused packages and provisioning files on the currently booted device will be cleaned. The currently booted device is where the committed `packages.conf` file resides.

### Examples

This example uses the 'software clean' command with no command options to clean the current boot directory, `flash:`, on a standalone switch that is running in installed mode.
infra-p2-3#dir flash:
Directory of flash:

7378 -rwx 2097152 Nov 15 2012 09:45:11 +00:00 nvram_config
7379 drwx 4096 Nov 15 2012 09:19:24 +00:00 mnt
7396 -rwx 1244 Nov 14 2012 18:32:55 +00:00 packages.conf.00-
7390 -rwx 74390300 Nov 15 2012 09:18:17 +00:00 cat3k_caa-base.SSA.03.09.16.EMD.pkg
7383 -rwx 74601776 Nov 14 2012 18:31:59 +00:00 cat3k_caa-base.SSA.03.09.16.EMP.pkg
7384 -rwx 2732724 Nov 14 2012 18:32:08 +00:00 cat3k_caa-drivers.SSA.03.09.16.EMP.pkg
7385 -rwx 49886128 Nov 14 2012 18:32:02 +00:00 cat3k_caa-drivers.SSA.03.09.16.EMD.pkg
7387 -rwx 30579500 Nov 14 2012 18:32:05 +00:00 cat3k_caa-infra.SSA.03.09.16.EMD.pkg
7386 -rwx 556 Nov 9 2012 09:58:21 +00:00 vlan.dat
7389 -rwx 62814928 Nov 14 2012 18:32:08 +00:00 cat3k_caa-wcm.SSA.03.09.16.EMD.pkg
7388 -rwx 18193120 Nov 14 2012 18:32:03 +00:00 cat3k_caa-platform.SSA.03.09.16.EMD.pkg
7397 -rwx 1243 Nov 15 2012 09:18:55 +00:00 packages.conf
7391 -rwx 2734772 Nov 15 2012 09:18:17 +00:00 cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
7392 -rwx 32465772 Nov 15 2012 09:18:24 +00:00 cat3k_caa-drivers.SSA.03.09.17.EMD.pkg
7393 -rwx 30384940 Nov 15 2012 09:18:35 +00:00 cat3k_caa-infra.SSA.03.09.17.EMD.pkg
7394 -rwx 18143968 Nov 15 2012 09:18:39 +00:00 cat3k_caa-platform.SSA.03.09.17.EMD.pkg
7395 -rwx 62638800 Nov 15 2012 09:18:51 +00:00 cat3k_caa-wcm.SSA.03.09.17.EMD.pkg

712413184 bytes total (208535552 bytes free)
infra-p2-3#
infra-p2-3#software clean
Preparing clean operation ...
[2]: Cleaning up unnecessary package files
[2]: No path specified, will use booted path flash:packages.conf
[2]: Cleaning flash:
[2]: Preparing packages list to delete ...
cat3k_caa-base.SSA.03.09.17.EMP.pkg
  File is in use, will not delete.
cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
  File is in use, will not delete.
cat3k_caa-infra.SSA.03.09.17.EMP.pkg
  File is in use, will not delete.
cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
  File is in use, will not delete.
cat3k_caa-platform.SSA.03.09.17.EMP.pkg
  File is in use, will not delete.
cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
  File is in use, will not delete.
packages.conf
  File is in use, will not delete.
[2]: Files that will be deleted:
cat3k_caa-base.SSA.03.09.16.EMP.pkg
cat3k_caa-drivers.SSA.03.09.16.EMP.pkg
cat3k_caa-infra.SSA.03.09.16.EMP.pkg
cat3k_caa-iosd-universalk9.SSA.150-9.16.EMP.pkg
cat3k_caa-platform.SSA.03.09.16.EMP.pkg
cat3k_caa-wcm.SSA.03.09.16.EMP.pkg
packages.conf.00-

[2]: Do you want to proceed with the deletion? [yes/no]: y
[2]: Clean up completed
infra-p2-3#
infra-p2-3#dir flash:
Directory of flash:/

7378 -rwx 2097152 Nov 15 2012 09:45:11 +00:00 nvram_config
7379 drwx 4096 Nov 15 2012 09:19:24 +00:00 mnt
7390 -rwx 74390300 Nov 15 2012 09:18:17 +00:00 cat3k_caa-base.SSA.03.09.17.EMP.pkg
7396 -rwx 556 Nov 9 2012 09:58:21 +00:00 vlan.dat
7397 -rwx 1243 Nov 15 2012 09:18:55 +00:00 packages.conf
7391 -rwx 2734772 Nov 15 2012 09:18:17 +00:00 cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
7392 -rwx 3245772 Nov 15 2012 09:18:24 +00:00 cat3k_caa-infra.SSA.03.09.17.EMP.pkg
cat3k_caa-iods-universalk9.SSA.150-9.17.EMP.pkg
7394 -rwx 18143968 Nov 15 2012 09:18:39 +00:00 cat3k_caa-platform.SSA.03.09.17.EMP.pkg
7395 -rwx 62638800 Nov 15 2012 09:18:51 +00:00 cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (447623168 bytes free)
infra-p2-3#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
<tr>
<td></td>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the <strong>auto-rollback</strong> command option of the <strong>software install</strong> command.</td>
</tr>
<tr>
<td></td>
<td>software expand</td>
<td>Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.</td>
</tr>
<tr>
<td></td>
<td>software install source switch</td>
<td>Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.</td>
</tr>
<tr>
<td></td>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.</td>
</tr>
</tbody>
</table>

**software commit**

To commit a package set that was installed using the **auto-rollback** command option of the **software install** command, use the **software commit** command in Privileged EXEC mode.

**software commit**[{switchnodes}][{verbose}]

**Syntax Description**

- **switchnodes**: (optional) specifies which switch(es) should perform the commit operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
| verbose | (optional) provides some additional info in the log files |

**Command Default**

No software package(s) will be committed by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3SE</td>
<td>This command was integrated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `software commit` command cancels the rollback timer, if it is running, and commits a software upgrade. A commit makes an upgrade, i.e., a package set, persistent. A committed package set will run after a node is reloaded.

**Examples**

This example uses the 'software install file' command with the 'auto-rollback' command option to install the bundle onto both switches in a stack via tftp. After the switches reload with the new software, the 'software commit' command is used to stop the rollback timer and commit the candidate package set.

```
infra-p2-3#software install file
45
Preparing install operation ...
[2]: Downloading file
[2]: Finished downloading file
[2]: Copying software from active switch 2 to switch 1
[2]: Finished copying software to switch 1
[1 2]: Starting install operation
[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[1 2]: Copying package files
[1 2]: Package files copied
[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[1 2]: Verifying and copying expanded package files to flash:
[1 2]: Verified and copied expanded package files to flash:
[1 2]: Starting compatibility checks
[1 2]: Finished compatibility checks
[1 2]: Starting application pre-installation processing
[1 2]: Finished application pre-installation processing
[1]: Old files list:
  Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
  Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

[2]: Old files list:
  Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
```
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

[1]: New files list:
  Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
  Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg

[2]: New files list:
  Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
  Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg

[1 2]: Creating pending provisioning file
[1 2]: Finished installing software. New software will load on reboot.
[1 2]: Setting rollback timer to 45 minutes

[1 2]: Do you want to proceed with reload? [yes/no]: y
[1]: Reloading
[2]: Pausing before reload

*Nov 15 10:24:24.891: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr: Received reload request for switch 1, reason User requested reload
*Nov 15 10:24:25.051: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr: Stack port 2 on switch 2 is down
*Nov 15 10:24:25.051: %STACKMGR-1-SWITCH_REMOVED: 2 stack-mgr: Switch 1 has been removed from the stack
*Nov 15 10:24:25.146: %REdundancy-3-STAnDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Nov 15 10:24:25.146: %REdundancy-5-PEER_MONITOR_EVENT: Active detected a standby removal (raw-event=PEER_NOT_PRESENT(3))
*Nov 15 10:24:25.146: %REdundancy-3-STAnDBY_LOST: Standby processor fault (PEER_DOWN)
*Nov 15 10:24:25.146: %REdundancy-5-PEER_MONITOR_EVENT: Active detected standby down or crashed (raw-event=PEER_DOWN(2))
*Nov 15 10:24:25.146: %REdundancy-3-STAnDBY_LOST: Standby processor fault (PEER_REDUNDANCY_STATE_CHANGE)
*Nov 15 10:24:25.146: %REdundancy-5-PEER_MONITOR_EVENT: Active detected a standby removal (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Nov 15 10:24:27.054: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Nov 15 10:24:28.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
[2]: Reloading
infra-p2-3#

infra-p2-3#show software installer rollback-timer
< Switches were reloaded and booted with the newly installed software>

*Nov 15 10:34:21.345: %AUTHMGR_SPI-6-START: Auth Manager SPI server started (infra-p2-3-1)
*Nov 15 10:34:24.612: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Nov 15 10:34:24.624: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Nov 15 10:34:24.510: %SSH-5-DISABLED: SSH 1.99 has been disabled (infra-p2-3-1)
*Nov 15 10:34:24.511: %SSH-5-ENABLED: SSH 1.99 has been enabled (infra-p2-3-1)
infra-p2-3#show software installer rollback-timer
Switch# Status Duration
----------------------------------
1 active 00:31:28
2 active 00:31:43

infra-p2-3#
infra-p2-3#show software installer rollback-timer
Switch# Status Duration
----------------------------------
1 inactive -
2 inactive -

infra-p2-3#
infra-p2-3#software commit
Preparing commit operation ...  
[1 2]: Starting commit operation 
[1 2]: Finished committing software changes.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that</td>
</tr>
<tr>
<td></td>
<td>are no longer in use.</td>
</tr>
<tr>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
<tr>
<td>software expand</td>
<td>Use this command to expand individual IOS XE Software packages and the</td>
</tr>
<tr>
<td></td>
<td>provisioning file from a specified bundle to a specific destination</td>
</tr>
<tr>
<td></td>
<td>directory.</td>
</tr>
<tr>
<td>software install source</td>
<td>Use this command to install the running IOS XE software packages from one</td>
</tr>
<tr>
<td>switch</td>
<td>stack member to one or more other stack members.</td>
</tr>
<tr>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a</td>
</tr>
<tr>
<td></td>
<td>previous installation point.</td>
</tr>
</tbody>
</table>

software expand

To expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory, use the software expand command in Privileged EXEC mode.

To expand the individual IOS XE Software packages and the provisioning file from the running bundle, use the software expand running command in Privileged EXEC mode.

software expand  {file source url [running][{to destination url}][{switchnodes}][{verbose}]}
### Syntax Description

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filesources</code></td>
<td>URL of the bundle to be expanded. If a network URL is specified, the <code>to</code> keyword must also be used to specify the destination location. The <code>file</code> and <code>running</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><code>running</code></td>
<td>Specifies that the packages from the running bundle should be expanded. The <code>to</code> keyword must also be used to specify the destination location. The <code>file</code> and <code>running</code> keywords are mutually exclusive. The running command option is not allowed when running in installed mode.</td>
</tr>
<tr>
<td><code>todeestination</code></td>
<td>Specifies the local or UFS directory where the expanded bundle contents are copied to.</td>
</tr>
<tr>
<td><code>switchnodes</code></td>
<td>(optional) Specifies which switch(es) should perform the expand operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.</td>
</tr>
<tr>
<td><code>verbose</code></td>
<td>(optional) Provides some additional info in the log files</td>
</tr>
</tbody>
</table>

### Command Default

Command is used to expand an IOS XE software bundle. The contents are extracted into the same directory as the source bundle by default.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
Release | Modification
--- | ---
Cisco IOS XE Release 3.3SE | This command was integrated.

**Usage Guidelines**

If the `to` option is not entered, the contents will be extracted into the default installation location for the platform.

The bundle file is unchanged after the operation is complete.

**Examples**

This example uses the following steps to prepare a switch for booting in installed mode, i.e., booting a package provisioning file (packages.conf)

1. Boot in bundle mode using `bootflash:<bundlename>`. Can also boot from usbflash0: or via tftp

   ```
   switch: b tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.17.EMP.150-9.17.EMP.bin
   ```

   Reading full image into memory ...

   Nova Bundle Image

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

   Kernel Address : 0x6042fef4
   Kernel Size : 0x317ccc/3243212
   Initramfs Address : 0x60747bc0
   Initramfs Size : 0xdbf2f9/14414585
   Compression Format: .mzip

   Bootable image at @ ram:0x6042fef4
   Bootable image segment 0 address range [0x8110000, 0x81b80000] is in range [0x80180000, 0x90000000].
   
   File "tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.17.EMP.150-9.17.EMP.bin" uncompressed and installed, entry point: 0x811060f0

   Loading Linux kernel with entry point 0x811060f0 ...
   Bootloader: Done loading app on core_mask: 0xf

   ### Launching Linux Kernel (flags = 0x5)

   All packages are Digitally Signed
   Starting System Services

   : 

   *Nov 15 10:49:35.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/1/1, changed state to down
   *Nov 15 10:49:35.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/1/2, changed state to down
   *Nov 15 10:49:36.822: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up
   infra-p2-3# 
   infra-p2-3>enable
   infra-p2-3#

2. Use the 'software clean file flash:' command to remove any unused package, bundle and provisioning files from flash:

   ```
   infra-p2-3#software clean file flash:
   Preparing clean operation ...
   [2]: Cleaning up unnecessary package files
   [2]: Preparing packages list to delete ...
   [2]: Files that will be deleted:
       cat3k_caa-base.SSA.03.09.19.EMP.pkg
       cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
   ```
cat3k_caa-infra.SSA.03.09.19.EMP.pkg
cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
infra-p2-3#

3. Use the 'software expand running to flash:' command to expand the running bundle to flash:

infra-p2-3# software expand running to flash:
Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle

infra-p2-3#
infra-p2-3# dir flash:
Directory of flash: /
7378 -rwx 2097152 Nov 15 2012 10:49:37 +00:00 nvram_config
14753 drwx 4096 Nov 15 2012 10:20:27 +00:00 mnt
7381 -rw- 74390300 Nov 15 2012 10:54:24 +00:00 cat3k_caa-base.SSA.03.09.17.EMP.pkg
7382 -rw- 2734772 Nov 15 2012 10:54:24 +00:00 cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
7383 -rw- 32465772 Nov 15 2012 10:54:24 +00:00 cat3k_caa-infra.SSA.03.09.17.EMP.pkg
7384 -rw- 30384940 Nov 15 2012 10:54:24 +00:00 cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
7385 -rw- 18143968 Nov 15 2012 10:54:24 +00:00 cat3k_caa-platform.SSA.03.09.17.EMP.pkg
7380 -rw- 1243 Nov 15 2012 10:55:03 +00:00 packages.conf
7386 -rwx 556 Nov 9 2012 09:58:21 +00:00 vlan.dat
7387 -rw- 62638800 Nov 15 2012 10:54:24 +00:00 cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
712413184 bytes total (447627264 bytes free)
infra-p2-3#

4. Reload the switch

infra-p2-3# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

* Nov 15 10:56:36:569: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr: Received reload request for all switches, reason Reload command
* Nov 15 10:56:36:570: %STACKMGR-1-RELOAD: 2 stack-mgr: reloading due to reason Reload command
* Nov 15 10:56:37.071: %IOSXE-3-PLATFORM: 2 process sysmgr: Reset/Reload requested by [stack-manager].
<Thu Nov 15 10:56:37 2012> Message from sysmgr: Reset Reason:Reset/Reload requested by [stack-manager]. [Reload command]

5. Boot the installed packages using 'boot flash:packages.conf'

switch: boot flash:packages.conf
Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74390300
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042f354
Kernel Size : 0x317ccc/3243212
Initramfs Address : 0x60747020
Initramfs Size : 0xdbf2f9/14414585
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range
[0x80180000, 0x90000000].
boot_system: 377
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)
All packages are Digitally Signed
Starting System Services
:
:

TenGigabitEthernet2/1/1, changed state to down
TenGigabitEthernet2/1/2, changed state to down
*Nov 15 11:05:24.286: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up

infra-p2-3>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that are no longer in use.</td>
</tr>
<tr>
<td></td>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
<tr>
<td></td>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the auto-rollback command option of the software install command.</td>
</tr>
<tr>
<td></td>
<td>software install source switch</td>
<td>Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.</td>
</tr>
<tr>
<td></td>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.</td>
</tr>
</tbody>
</table>

**software install file**

To install IOS XE Software files, use the **software install file** command in Privileged EXEC mode.
**software install file**  
`bundle url`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file <code>bundle url</code></td>
<td>Specify the url of the bundle file to be installed.</td>
</tr>
<tr>
<td>switch nodes</td>
<td>(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.</td>
</tr>
<tr>
<td>auto-rollback minutes</td>
<td>(optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit'). If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software).</td>
</tr>
<tr>
<td>on-reboot</td>
<td>(optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages.</td>
</tr>
<tr>
<td>provisioning-file <code>provisioning-file url</code></td>
<td>(optional) Specifies the provisioning file to be updated by the installation. Default is the running provisioning file. Valid locations are flash: or usbflash0:</td>
</tr>
</tbody>
</table>
**Command Default**

Command is used to install IOS XE software. No software will be installed by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3SE</td>
<td>This command was integrated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **software install file** command is used to install package files from a software bundle when the system is running in installed mode. By default, the command will install software on all nodes in the system.

The following tasks are performed during the **software install file** operation:

- For a network installation, download the specified software bundle into memory on the active node (or standalone node is a standalone system).

- In a multi-node system, copy the software bundle to each node if the file does not already exist on the node. If installing a bundle that resides in local media on the active node (flash: or usbfash0:), the bundle file (.bin) is copied to the corresponding local device on each node. If installing a bundle via the network, the bundle is copied to memory on each node in the system.

- Expand the package files from the specified bundle into flash: on each node after verifying each package's digital signature.

---

**Table**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force</td>
<td>(optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.</td>
</tr>
<tr>
<td>new</td>
<td>(optional) Indicates that the post-install package set should contain only the packages being installed. Without this option, the post-install package set is a merged set of the currently installed software and the new packages being installed.</td>
</tr>
<tr>
<td>verbose</td>
<td>(optional) provides some additional info in the log files</td>
</tr>
</tbody>
</table>
- Perform compatibility checks on all nodes in the system to ensure that the software running on all nodes after installation will be compatible. This task is skipped if the force command option is used.

- Start the auto-rollback timer if the auto-rollback command option was used. The newly installed packages will be automatically rolled back if the auto-rollback timer expires before the 'software commit' command is issued.

- Update the package provisioning file (packages.conf) and save a copy of the original provisioning file for use during auto-rollback or user-initiated rollback (software rollback command).

- Commit the newly installed software packages if the auto-rollback command option was not used.

- Prompt the user to reload (if the on-reboot command option was not used).

Note: The software install file command cannot be used if the system is running in bundle mode. In this case, the software expand command can be used to prepare the system to boot in installed mode.

Examples

The following example installs the cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin bundle from a tftp server. The bundle is first downloaded to RAM, then the package files included in the bundle are extracted and copied to flash:. The .bin file itself is not copied to flash:

Preparing install operation ...
[2]: Downloading file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Finished downloading file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Starting install operation
[2]: Copying package files
[2]: Package files copied
[2]: Verifying and copying expanded package files to flash:
[2]: Verified and copied expanded package files to flash:
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
  Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
  Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
  Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
  Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
  Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
  Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg

Note: You need IOSd IP connectivity to install via tftp.
[2]: Creating pending provisioning file
[2]: Finished installing software. New software will load on reboot.
[2]: Committing provisioning file

[2]: Do you want to proceed with reload? [yes/no]: n

infra-p2-3#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that are no longer in use.</td>
</tr>
<tr>
<td></td>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the auto-rollback command option of the software install command.</td>
</tr>
<tr>
<td></td>
<td>software expand</td>
<td>Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.</td>
</tr>
<tr>
<td></td>
<td>software install source switch</td>
<td>Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.</td>
</tr>
<tr>
<td></td>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.</td>
</tr>
</tbody>
</table>

**software install source switch**

To install the running IOS XE software packages from one stack member to one or more other stack members, use the `software install source switch` command in Privileged EXEC mode.

```
software install source switch node
[ {switchnode} ] [ {auto-rollback minutes} ] [ {force} ] [ {on-reboot} ] [ {verbose} ] [ {new} ] [ {provisioning-file provisioning-file-url} ]
```

**Syntax Description**

<p>| Syntax Description | switchnode | Specifies which switch in the stack to use as the package source. Only a single switch may be specified and there is no default value. |</p>
<table>
<thead>
<tr>
<th><strong>switch nodes</strong></th>
<th>(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.</th>
</tr>
</thead>
</table>
| **auto-rollback minutes**     | (optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit').  
If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software). |
| **force**                     | (optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities.  
Force should not generally be required, and should be used with caution.  
Local package compatibility checks are enforced regardless of this command option. |
| **on-reboot**                 | (optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages. |
| **verbose**                   | (optional) provides some additional info in the log files |
The `software install source switch` command is used to install the running package files from one stack member to one or more other stack members while the system is running in installed mode.

The following tasks are performed during the `software install source switch` operation.

- Copy the running software packages from flash: on the specified source switch to flash: on all other switches specified in the command.
- Perform compatibility checks on all switches in the stack to ensure that the software running on all stack members after installation will be compatible. This task is skipped if the `force` command option is used.
- Start the auto-rollback timer if the `auto-rollback` command option was used. The newly installed packages will be automatically rolled back if the auto-rollback timer expires before the `software commit` command is issued.
- Update the package provisioning file (packages.conf) and save a copy of the original provisioning file for use during auto-rollback or user-initiated rollback (`software rollback` command).
- Commit the newly installed software packages if the `auto-rollback` command option was not used.
- Prompt the user to reload (if the `on-reboot` command option was not used).

The `software install source switch` command cannot be used if the system is running in bundle mode. In this case, the `software expand` command can be used to prepare the system to boot in installed mode.
In the following example, the switches in a 2-member stack are running different (but compatible) software packages. The software install source switch command is used to install the currently running packages on the standby switch (switch 1) to the active switch (switch 2).

```
infra-p2-3#show version running
Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: IOS, version: 03.09.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi

infra-p2-3#software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2
[2]: Starting install operation
[2]: Starting compatibility checks
```
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
   Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
   Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
   Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
   Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
   Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
   Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
   Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
   Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
   Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
   Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
   Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
   Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software. New software will load on reboot.
[2]: Committing provisioning file
[2]: Do you want to proceed with reload? [yes/no]: no
infra-p2-3#

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that are no longer in use.</td>
</tr>
<tr>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
<tr>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the <code>auto-rollback</code> command option of the <code>software install</code> command.</td>
</tr>
<tr>
<td>software expand</td>
<td>Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.</td>
</tr>
<tr>
<td>software rollback</td>
<td>Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.</td>
</tr>
</tbody>
</table>

---

**software install source switch**

To install IOS XE Software objects from various sources, use the `software install source switch` command in Privileged EXEC mode.

```bash
software install source switch node [{switch nodes}][{auto-rollback minutes}] [{on-reboot}] [{provisioning-file provisioning-file-url}][{force}][{verbose}][{new}]
```
### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>source switch node</strong></td>
<td>Specifies which switch in the stack to use as the package source. Only a single switch may be specified and there is no default value.</td>
</tr>
<tr>
<td><strong>switch nodes</strong></td>
<td>(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.</td>
</tr>
<tr>
<td><strong>auto-rollback minutes</strong></td>
<td>(optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit'). If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software).</td>
</tr>
<tr>
<td><strong>on-reboot</strong></td>
<td>(optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages.</td>
</tr>
<tr>
<td><strong>provisioning-file provisioning-file-url</strong></td>
<td>(optional) Specifies the provisioning file to be updated by the installation. Default is the running provisioning file. Valid locations are flash: or usbflash0:</td>
</tr>
</tbody>
</table>
**force**

(optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities.

Force should not generally be required, and should be used with caution.

Local package compatibility checks are enforced regardless of this command option.

**new**

(optional) Indicates that the post-install package set should contain only the packages being installed.

Without this option, the post-install package set is a merged set of the currently installed software and the new packages being installed.

**verbose**

(optional) provides some additional info in the log files

---

**Command Default**

Command is used to install IOS XE software. No software will be installed by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3SE</td>
<td>This command was integrated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the **package** option is not specified, it means operate on (ie. upgrade) the currently provisioned packages using all of the packages from the input. If one or more package names *are* specified, they act as a filter on the input file set, limiting the upgrade to the given packages.

If one or more **switch** keywords are not specified, to identify destination node(s), then 'all' nodes are assumed as the destination.

If the **on-reboot** option is not specified, then the **software install file** command will do everything that the platform requires to make the specified packages "run", ie. to commit and activate them. This typically involves a system reload.

A new set of packages installed together succeed or fail together. Any one failure, on any node, fails the entire installation. As an example, using the "one-button" install (one single command to perform the upgrade):

```
software install file
<bundle-url>
```
Where the bundle contains 3 packages. The 3 packages will be expanded on to the box, on each node (in a multimode system). A new `candidate packages.conf` will be created with the 3 new packages added/changed (on each node). The packages in the new `candidate packages.conf` will be checked for compatibility. Then they will be activated together, on each node, in parallel.

If there is a failure at any point, or if the rollback timer is let to expire, the system will be rolled back to the state before the install command was issued.

**Examples**

To take advantage of the created source list, in exec mode use this command:

```plaintext
software install source
list <list-name> [package <package-name-or-wildcard>] [switch <node>]
[auto-rollback <minutes>] [force] [on-reboot] [verbose] [new]
```

All of the same options as for the 'software source url' command apply (as above).

Using the previous example, the installation command to install *all* of the packages using the above named list would be:

```plaintext
software install source list my-list-123
```

with any options, as required. This is equivalent to entering:

```plaintext
software install source list my-list-123 package *
```

The default argument for 'package' is therefore '*' (for the software install source list command). As another example, to install all "wcm" packages from the same list:

```plaintext
software install source list my-list-123 package *wcm*
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>software install file</code></td>
<td>Install Cisco IOS XE files.</td>
</tr>
</tbody>
</table>

**software provision**

To organize IOS XE Software packages from an input bundle(s) or a list onto a flash device for later activation, use the `software provision` command in Privileged EXEC mode.

```plaintext
software provision source {url bundle or package url | list/list-name} [{package package name or wildcard}] [{switch/node}] [{force}] [{verbose}]```

**Syntax Description**

<table>
<thead>
<tr>
<th>list/list-name</th>
<th>Specify an ordered list of input bundles of directories to provision.</th>
</tr>
</thead>
<tbody>
<tr>
<td>package</td>
<td>Specify the package filenames to be provisioned.</td>
</tr>
</tbody>
</table>
### bundle or package url
Specify a bundle or package(s) to be installed. A wildcard may be used to specify the input, but only one bundle is accepted (as the end result of the wildcard operation). By contrast, more than one package file will be accepted as the result of a wildcard operation.

### switch
Indicates a particular node, an independent instance running Nova, to which the operation will be performed.

### force
Specifies that the operation will proceed despite any remote package incompatibilities, without interacting with the user.

**Note** Force should not generally be required for upgrades, and should be used with caution. Local package compatibilities are always enforced.

### verbose
Displays all output that can be displayed on the console during the operation.

---

**Command Default**
No software will be provisioned by default.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **software provision** command does not activate nor commit any copied packages. This provisioning command effectively builds up a list of packages into a `candidate packages.conf` file, which forms the input for the **software activate** command.

The **software provision** command may be run multiple times in order to "build up" a desired set of packages for upgrade. The package set is built up into an internal `candidate packages.conf` file, and the packages become "installed pending activation".

**Examples**
To:
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>software activate</code></td>
<td>Activates provisioned Cisco IOS XE files.</td>
</tr>
</tbody>
</table>

---

**software repackage**

To take a snapshot of a committed Cisco IOS XE Software package and create a bundle from it to be copied off-box, use the `software repackage` command in Privileged EXEC mode.

```
software repackage  switch node dest url and filename
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch</code></td>
<td>Indicates a particular node, an independent instance running Nova, from which the particular package will be repackaged.</td>
</tr>
<tr>
<td><code>destination url and filename</code></td>
<td>Specifies the destination location for the repackaged bundle.</td>
</tr>
</tbody>
</table>

**Command Default**

No software will be repackaged by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The installer can repack a set of committed packages, and copy them off-box to any arbitrary filesystem. This takes a snapshot of the committed software and creates a bundle from it.

**Examples**

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>software install source url</code></td>
<td>This command is an alternative to 'software install file' that allows some packages from a bundle, but not all of the packages, to be installed, if desired.</td>
</tr>
<tr>
<td><code>software install source list</code></td>
<td>Use this command to install a list of input bundles or directories.</td>
</tr>
<tr>
<td><code>software install source switch</code></td>
<td>Use this command to install from one node to another.</td>
</tr>
</tbody>
</table>

---

**software rollback**

To roll back the committed Cisco IOS XE Software to a previous installation point, use the `software rollback` command in Privileged EXEC mode.

```
software rollback [{switch node}] [{as-booted}] [{provisioning-file source}] [{url}] [{on-reboot}] [{force}] [{verbose}]
```
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switchnodes</code></td>
<td>(optional) specifies which switch(es) should perform the rollback operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.</td>
</tr>
<tr>
<td><code>as-booted</code></td>
<td>(optional) Used to rollback any installations that have occurred since bootup and commit the booted packages.conf file.</td>
</tr>
<tr>
<td><code>provisioning-file</code></td>
<td>(optional) Specifies the provisioning file to be updated by the rollback. Default is the running provisioning file. Valid locations are flash: or usbflash0:</td>
</tr>
<tr>
<td><code>on-reboot</code></td>
<td>(optional) Indicates that the user should not prompted to reload when the rollback operation completes. The user must then use the reload command to boot the system with the newly installed packages.</td>
</tr>
<tr>
<td><code>force</code></td>
<td>(optional) Specifies that the operation will be forced. Forced means that the rollback will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.</td>
</tr>
<tr>
<td><code>verbose</code></td>
<td>(optional) provides some additional info in the log files</td>
</tr>
</tbody>
</table>

### Command Default

No software will be rolled-back by default.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3.SE</td>
<td>This command was integrated.</td>
</tr>
</tbody>
</table>
The `software rollback` command rolls back the committed software, ie. set of packages, to a previous installation point.

The software rollback functionality relies on the existence of one or more rollback provisioning files in flash; along with all of the .pkg files listed in the rollback provisioning file(s).

The rollback provisioning files are visible in flash: as packages.conf.00-, packages.conf.01-, etc.

- packages.conf.00- is a snapshot of the packages.conf file as it looked prior to the last installation operation.
- packages.conf.01- is a snapshot of the packages.conf file as it looked two installations ago. (This pattern continues for all provisioning files.)

When the `software rollback` command is used, packages.conf.00- becomes packages.conf, packages.conf.01- becomes packages.conf.00-, etc.

If the `software clean` command is used, future attempts to do a software rollback will fail if the rollback provisioning file and/or the packages listed in it have been cleaned.

This example uses the 'software rollback' command to revert to the previously installed package set (packages.conf.00-).

```
infra-p2-3#software rollback
Preparing rollback operation ...
[2]: Starting rollback operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
  Removed cat3k_caa-base.SSA.03.09.19.EMP.pkg
  Removed cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
  Removed cat3k_caa-infra.SSA.03.09.19.EMP.pkg
  Removed cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
  Removed cat3k_caa-platform.SSA.03.09.19.EMP.pkg
  Removed cat3k_caa-wcm.SSA.03.09.19.EMP.pkg

[2]: New files list:
  Added cat3k_caa-base.SSA.03.09.17.EMP.pkg
  Added cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
  Added cat3k_caa-infra.SSA.03.09.17.EMP.pkg
  Added cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
  Added cat3k_caa-platform.SSA.03.09.17.EMP.pkg
  Added cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

[2]: Creating pending provisioning file
[2]: Finished rolling back software changes. New software will load on reboot.

[2]: Do you want to proceed with reload? [yes/no]: n
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software clean</td>
<td>Use this command to remove any and all packages and provisioning files that are no longer in use.</td>
</tr>
</tbody>
</table>
### Command Table

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software install file</td>
<td>Install Cisco IOS XE files.</td>
</tr>
<tr>
<td>software commit</td>
<td>Use this command to commit a package set that was installed using the auto-rollback command option of the software install command.</td>
</tr>
<tr>
<td>software expand</td>
<td>Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.</td>
</tr>
<tr>
<td>software install source switch</td>
<td>Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.</td>
</tr>
</tbody>
</table>

### software source list

To create a list of input bundles or directories, use the `software source list` command in global configuration mode.

**Syntax**

```
software source list  list-name-string
```

To erase a source list, use the `no` form of the `software source list` command.

**no software source list  list-name-string**

**Syntax Description**

<table>
<thead>
<tr>
<th>list-name-string</th>
<th>Name of the list or string.</th>
</tr>
</thead>
</table>

**Command Default**

No source list exists.

**Command Modes**

Global configuration (config)

**Command History**

Release | Modification
---------|--------------|

**Usage Guidelines**

If it happens that using either the `software install file` command or the `software install source` commands result in an error due to too many characters on the command line, you can create a list of input bundles or directories using the `software source list` command.

The available configured lists may then be verified using the `show running config` command, which also displays the contents of the lists. The pool of packages defined by a list can be displayed with the `show software source list list-name` command.

**Examples**

To create a source list named "my-list-123" perform the following
This effectively creates a pool of packages from which to find ("source"), a package. It creates an ordered search list for Installer to find a given package. For example, a requested package will first be looked for in the bundle file 'tftp://my-big-bundle.bin'. If not found, the requested package will then be looked for in the directory. Naturally, packages would have had to have been previously 'expanded' into the directory 'bootflash:/packages1' by the user to make them available for use in this manner.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>software install file</td>
<td>Install IOS XE software files.</td>
</tr>
<tr>
<td>software install source</td>
<td>Install IOS XE software from a given source.</td>
</tr>
</tbody>
</table>

### software uninstall

To deactivate a Cisco IOS XE Software package or set of packages, use the `software uninstall` command in Privileged EXEC mode.

```
software uninstall  bundle or package url [{switchnode}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>bundle or package url</th>
<th>Specify a bundle or package(s) to be deactivated.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong> Wildcards may be used</td>
</tr>
<tr>
<td>switch</td>
<td>Indicates a particular node, an independent instance running Nova, from which the particular package will be uninstalled.</td>
</tr>
</tbody>
</table>

**Command Default**

No software will be uninstalled by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Wildcards can be used with the 'package' argument.

**Note**

There may be restrictions on what can be uninstalled. For example, the installer will refuse to uninstall a package where there is no compatible ancestor.
special-character-bits

To configure the number of data bits per character for special characters such as software flow control characters and escape characters, use the `special-character-bits` command in line configuration mode. To restore the default value, use the `no` form of this command.

```sh
special-character-bits {7|8}
no special-character-bits
```

**Syntax Description**

- 7: Selects the 7-bit ASCII character set. This is the default.
- 8: Selects the full 8-bit character set for special characters.

**Command Default**

7-bit ASCII character set

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Setting the special character bits to 8 allows you to use twice as many special characters as with the 7-bit ASCII character set. The special characters affected by this setting are the escape, hold, stop, start, disconnect, and activation characters.

**Examples**

The following example allows the full 8-bit international character set for special characters on line 5:

```sh
Router(config)# line 5
Router(config-line)# special-character-bits 8
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-value exec-character-bits</td>
<td>Defines the EXEC character width for either 7 bits or 8 bits.</td>
</tr>
<tr>
<td>default-value special-character-bits</td>
<td>Configures the flow control default value from a 7-bit width to an 8-bit width.</td>
</tr>
<tr>
<td>exec-character-bits</td>
<td>Configures the character widths of EXEC and configuration command characters.</td>
</tr>
<tr>
<td>terminal exec-character-bits</td>
<td>Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.</td>
</tr>
<tr>
<td>terminal special-character-bits</td>
<td>Changes the ASCII character widths to accept special characters for the current terminal line and session.</td>
</tr>
</tbody>
</table>

### squeeze

To permanently erase files tagged as “deleted” or “error” on Class A flash file systems, use the `squeeze` command in privileged EXEC mode.

```
squeeze [/nolog] [/quiet] filesystem:
```

**Cisco 7600 Series Router**

`squeeze filesystem:`

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/nolog</td>
<td>(Optional) Disables the squeeze log (recovery data) and accelerates the squeeze process.</td>
</tr>
<tr>
<td>/quiet</td>
<td>(Optional) Disables status messages during the squeeze process.</td>
</tr>
<tr>
<td>filesystem</td>
<td>The flash file system, followed by a colon. For the Cisco 7600 series router, the valid values for the flash file system are <code>bootflash:</code> and <code>flash:</code></td>
</tr>
</tbody>
</table>

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(1)</td>
<td>This command was implemented on the Cisco 2600 and Cisco 3600 series routers.</td>
</tr>
<tr>
<td>12.0(17)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(17)S, and the <code>/nolog</code> and <code>/quiet</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(1a)</td>
<td>The <code>/nolog</code> and <code>/quiet</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(17)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(17)ST.</td>
</tr>
<tr>
<td>12.1(9)E</td>
<td>This command was integrated into Cisco IOS Release 12.1(9)E.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)B</td>
<td>This command was integrated into Cisco IOS Release 12.2(2)B.</td>
</tr>
<tr>
<td>12.2(4)XL</td>
<td>This command was implemented on the Cisco 1700 series routers.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was integrated into Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When flash memory is full, you might need to rearrange the files so that the space used by the files marked “deleted” can be reclaimed. (This “squeeze” process is required for linear flash memory cards to make sectors contiguous; the free memory must be in a “block” to be usable.)

When you enter the `squeeze` command, the router copies all valid files to the beginning of flash memory and erases all files marked “deleted.” After the squeeze process is completed, you can write to the reclaimed flash memory space.

⚠️

Caution

After performing the squeeze process, you cannot recover deleted files using the `undelete` EXEC mode command.

In addition to removing deleted files, use the `squeeze` command to remove any files that the system has marked as “error”. An error file is created when a file write fails (for example, the device is full). To remove error files, you must use the `squeeze` command.

Rewriting flash memory space during the squeeze operation may take several minutes.

Using the `/nolog` keyword disables the log for the squeeze process. In most cases, this process will speed up the squeeze process. However, if power is lost or the flash card is removed during the squeeze process, all the data on the flash card will be lost, and the device will have to be reformatted.

✏️

Note

Using the `/nolog` keyword makes the squeeze process uninterruptible.

Using the `/quiet` keyword disables the output of status messages to the console during the squeeze process.

If the optional keywords are not used, the progress of the squeeze process will be displayed to the console, a log for the process will be maintained, and the squeeze process is interruptible.

On Cisco 2600 or Cisco 3600 series routers, the entire file system has to be erased once before the `squeeze` command can be used. After being erased once, the `squeeze` command should operate properly on the flash file system for the rest of the flash file system’s history.

To erase an entire flash file system on a Cisco 2600 or 3600 series router, perform the following steps:

1. If the flash file system has multiple partitions, enter the `no partition` command to remove the partitions. The reason for removing partitions is to ensure that the entire flash file system is erased. The `squeeze` command can be used in a flash file system with partitions after the flash file system is erased once.

2. Enter the `erase` command to erase the flash file system.
Examples

Supported Platforms Other than the Cisco 7600 Series Router

In the following example, the file named config1 is deleted, and then the `squeeze` command is used to reclaim the space used by that file. The `/nolog` option is used to speed up the squeeze process.

Router# delete config1
Delete filename [config1]?
Delete slot0:conf? [confirm]
Router# dir slot0:

! Note that the deleted file name appears in square brackets
Directory of slot0:/
  1 -rw- 4300244 Apr 02 2001 03:18:07 c7200-boot-mz.122-0.14
  2 -rw-  2199 Apr 02 2001 04:45:15 [config1]
  3 -rw- 4300244 Apr 02 2001 04:45:23 image
20578304 bytes total (11975232 bytes free)
120,578,304 - 4,300,244 - 4,300,244 - 2,199 - 385 = 11975232
Router# squeeze /nolog slot0:

%Warning: Using /nolog option would render squeeze operation uninterruptible.
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Squeeze of slot0 completed in 291.832 secs.
Router# dir slot0:

Directory of slot0:/
  1 -rw- 4300244 Apr 02 2001 03:18:07 c7200-boot-mz.122-0.14
  2 -rw- 4300244 Apr 02 2001 04:45:23 image
20578304 bytes total (11977560 bytes free)
120,578,304 - 4,300,244 - 4,300,244 - 256 = 11977560

Cisco 7600 Series Router

This example shows how to permanently erase the files that are marked “deleted” from the flash memory:

Router#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Deletes a file on a flash memory device.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td>erase</td>
<td>Erases a file system.</td>
</tr>
<tr>
<td>undelete</td>
<td>Recovers a file marked “deleted” on a Class A or Class B flash file system.</td>
</tr>
</tbody>
</table>

stack-mib portname

To specify a name string for a port, use the `stack-mib portname` command in interface configuration mode.
stack-mib  portname  portname

**Syntax Description**

| portname | Name for a port. |

**Command Default**

This command has no default settings.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2917d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using the `stack-mib` command to set a name string to a port corresponds to the portName MIB object in the portTable of CISCO-STACK-MIB. portName is the MIB object in the portTable of CISCO-STACK-MIB. You can set this object to be descriptive text describing the function of the interface.

**Examples**

This example shows how to set a name to a port:

```
Router(config-if) #
stack-mib portname portall
Router(config-if) #
```

---

**state-machine**

To specify the transition criteria for the state of a particular state machine, use the `state-machine` command in global configuration mode. To remove a particular state machine from the configuration, use the `no` form of this command.

```
state-machine name state first-character last-character [{next-state [delay|transmit]}]
no state-machine name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>Name for the state machine (used in the <code>dispatch-machine</code> line configuration command). The user can specify any number of state machines, but each line can have only one state machine associated with it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>State being modified. There are a maximum of eight states per state machine. The range is from 0 to 7. Lines are initialized to state 0 and return to state 0 after a packet is transmitted.</td>
</tr>
</tbody>
</table>
A range of characters. Use ASCII numerical values. The range is from 0 to 255. If the state machine is in the indicated state, and the next character input is within this range, the process goes to the specified next state. Full 8-bit character comparisons are performed, so the maximum value is 255. Ensure that the line is configured to strip parity bits (or not generate them), or duplicate the low characters in the upper half of the space.

(Optional) State to enter if the character is in the specified range. The range is from 0 to 7.

(Optional) Transmits the packet if there is no input within 50 milliseconds.

(Optional) Causes the packet to be transmitted and the state machine to be reset to state 0. Recurring characters that have not been explicitly defined to have a particular action return the state machine to state 0.

No transition criteria are specified.

Global configuration (config)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The delay keyword was added.</td>
</tr>
</tbody>
</table>

This command is paired with the dispatch-machine line configuration command, which defines the line on which the state machine is effective.

In the following example a dispatch machine named “function” is configured to ensure that the function key characters on an ANSI terminal are kept in one packet. Because the default in the example is to remain in state 0 without sending anything, normal key signals are sent immediately.

```
Router(config)# line 1 20
Router(config-line)# dispatch-machine function
Router(config-line)# exit
Router(config)# state-machine function 0 0 255 6 transmit
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dispatch-character</td>
<td>Defines a character that causes a packet to be sent.</td>
</tr>
<tr>
<td>dispatch-machine</td>
<td>Specifies an identifier for a TCP packet dispatch state machine on a particular line.</td>
</tr>
<tr>
<td>dispatch-timeout</td>
<td>Sets the character dispatch timer.</td>
</tr>
</tbody>
</table>
**stopbits**

To set the number of the stop bits transmitted per byte, use the **stopbits** command in line configuration mode. To restore the default value, use the **no** form of this command.

```plaintext
stopbits \{1|1.5|2\}
no stopbits
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>One stop bit.</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>One and one-half stop bits.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Two stop bits. This is the default.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

2 stop bits per byte

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.

**Examples**

In the following example, the stop bits transmitted per byte are changed from the default of two stop bits to one stop bit as a performance enhancement for line 4:

```plaintext
Router(config)# line 4
Router(config-line)# stopbits 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal stopbits</td>
<td>Changes the number of stop bits sent per byte by the current terminal line during an active session.</td>
</tr>
</tbody>
</table>

**storm-control level**

To set the suppression level, use the **storm-control level** command in interface configuration mode. To turn off the suppression mode, use the **no** form of this command.

```plaintext
storm-control \{broadcast|multicast|unicast\} level level [.. level]
no storm-control \{broadcast|multicast|unicast\} level
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td></td>
<td>Specifies the broadcast traffic.</td>
</tr>
</tbody>
</table>
storm-control level

| multicast | Specifies the multicast traffic. |
| unicast   | Specifies the unicast traffic.   |
| level     | Integer-suppression level; valid values are from 0 to 100 percent. |
|           | (Optional) Fractional-suppression level; valid values are from 0 to 99. |

**Command Default**
All packets are passed.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You can enter this command on switch ports and router ports.

Enter the `storm-control level` command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

Only one suppression level is shared by all three suppression modes. For example, if you set the broadcast level to 30 and set the multicast level to 40, both levels are enabled and set to 40.

The Cisco 7600 series router supports storm control for multicast and unicast traffic only on Gigabit Ethernet LAN ports. The switch supports storm control for broadcast traffic on all LAN ports.

The `multicast` and `unicast` keywords are supported on Gigabit Ethernet LAN ports only. These keywords are not supported on 10 Mbps, 10/100 Mbps, 100 Mbps, or 10-Gigabit Ethernet modules.

The period is required when you enter the fractional-suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port, with the following guidelines:

- A fractional level value of 0.33 or lower is the same as 0.0 on the following modules:
  - WS-X6704-10GE
  - WS-X6748-SFP
  - WS-X6724-SFP
  - WS-X6748-GE-TX

- A fractional level value of 0.29 or lower is the same as 0.0 on the WS-X6716-10G-3C / 3CXL in Oversubscription Mode.

- Enter 0 on all other modules to block all specified traffic on a port.

Enter the `show interfaces counters broadcast` command to display the discard count.

Enter the `show running-config` command to display the enabled suppression mode and level setting.
To turn off suppression for the specified traffic type, you can do one of the following:

- Set the level to 100 percent for the specified traffic type.
- Use the no form of this command.

### Examples

This example shows how to enable and set the suppression level:

```bash
Router(config-if)#
storm-control broadcast level 30
```

This example shows how to disable the suppression mode:

```bash
Router(config-if)#
no storm-control multicast level
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces counters</td>
<td>Displays the traffic that the physical interface sees.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>

### sync-restart-delay

To set the synchronization-restart delay timer to ensure accurate status reporting, use the `sync-restart-delay` command in interface configuration mode. To disable the synchronization-restart delay timer, use the `no` form of this command.

```plaintext
sync-restart-delay timer
no sync-restart-delay timer
```

#### Syntax Description

- `timer` Interval between status-register resets; valid values are from 200 to 60000 milliseconds.

#### Command Default

- `timer` is 210 milliseconds.

#### Command Modes

- Interface configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- This command is supported on Gigabit Ethernet fiber ports only.
- The status register records the current status of the link partner.
Examples

This example shows how to set the Gigabit Ethernet synchronization-restart delay timer:

Router(config-if)# sync-restart-delay 2000

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the status and configuration of the module or Layer 2 VLAN.</td>
</tr>
</tbody>
</table>

systat

Note

This command has been replaced by the `show users` command.

To display information about the active lines on the router, use the `systat` command in user EXEC or privileged EXEC mode.

`systat all`

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all lines, regardless of whether the lines are used or not.</td>
</tr>
</tbody>
</table>

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to display the active lines:

Router# systat
Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
Interface User Mode Idle Peer Address

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show users</td>
<td>Displays information about the active lines on the router.</td>
</tr>
</tbody>
</table>
system flowcontrol bus

To set the FIFO overflow error count, use the system flowcontrol bus command in global configuration mode. To return to the original FIFO threshold settings, use the no form of this command.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[default] system flowcontrol bus {auto</td>
<td>on}</td>
</tr>
<tr>
<td>no system flowcontrol bus</td>
<td>Specifies the original FIFO threshold settings.</td>
</tr>
</tbody>
</table>

Command Default

auto

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXF</td>
<td>Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

We recommend that you leave the system flow control in auto mode and use the other modes under the advice of Cisco TAC only.

Examples

This example shows how to monitor the FIFO overflow error count and send a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals:

```plaintext
Router(config)# system flowcontrol bus auto
```

This example shows how to specify the original FIFO threshold settings:

```plaintext
Router(config)# system flowcontrol bus on
```

system jumbomtu

To set the maximum size of the Layer 2 and Layer 3 packets, use the system jumbomtu command in global configuration mode. To revert to the default MTU setting, use the no form of this command.

system jumbomtu mtu-size
no system jumbomtu
**Syntax Description**

```
mtu-size | Maximum size of the Layer 2 and Layer 3 packet s; valid values are from 1500 to 9216 bytes.
```

**Command Default**

`mtu-size` is **9216** bytes.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mtu-size` parameter specifies the Ethernet packet size, not the total Ethernet frame size. The Layer 3 MTU is changed as a result of entering the `system jumbo mtu` command.

The `system jumbo mtu` command enables the global MTU for port ASICs. On a port ASIC after jumbo frames are enabled, the port ASIC accepts any size packet on the ingress side and checks the outgoing packets on the egress side. The packets on the egress side that exceed the global MTU are dropped by the port ASIC.

For example, if you have port A in VLAN 1 and Port B in VLAN 2, and if VLAN 1 and VLAN 2 are configured for `mtu 9216` and you enter the `system jumbo mtu 4000` command, the packets that are larger than 4000 bytes are not transmitted out because Ports B and A drop anything larger than 4000 bytes.

**Examples**

This example shows how to set the global MTU size to 1550 bytes:

```
Router(config)# system jumbo mtu 1550
```

This example shows how to revert to the default MTU setting:

```
Router(config)# no system jumbo mtu
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtu</td>
<td>Adjusts the maximum packet size or MTU size.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays traffic that is seen by a specific interface.</td>
</tr>
<tr>
<td>show system jumbo mtu</td>
<td>Displays the global MTU setting.</td>
</tr>
</tbody>
</table>

## tdm clock priority

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the Cisco AS5350, AS5400, and AS5850 access servers, use the `tdm clock priority` command in global configuration mode. To return the clock source and priority to the default values, use the `no` form of this command.

```
tdm clock priority priority-number {slot/ds1-port|slot/ds3-port:ds1-port|external|freerun}
no tdm clock priority priority-number {slot/ds1-port|slot/ds3-port:ds1-port|external|freerun}
```
**Syntax Description**

<table>
<thead>
<tr>
<th><strong>Priority</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-number</td>
<td>Priority of the clock source. The priority range is from 1 to 99. A clock set to</td>
</tr>
<tr>
<td></td>
<td>priority 100 will not drive the TDM bus.</td>
</tr>
<tr>
<td>slot / ds1-port</td>
<td>Trunk-card slot is a value from 1 to 7. DS1 port number controller is a value</td>
</tr>
<tr>
<td></td>
<td>between 0 and 7. Specify with a slash separating the numbers; for example, 1/1.</td>
</tr>
<tr>
<td>slot / ds3-port : ds1-port</td>
<td>Trunk-card slot is a value from 1 to 7. DS3 port specifies the T3 port. DS1 port number controller is a value from 1 to 28. Specify with a slash separating the slot and port numbers, and a colon separating the DS1 port number. An example is 1/0:19.</td>
</tr>
<tr>
<td>external</td>
<td>Synchronizes the TDM bus with an external clock source that can be used as an</td>
</tr>
<tr>
<td></td>
<td>additional network reference.</td>
</tr>
<tr>
<td>freerun</td>
<td>Selects the free-running clock from the local oscillator when there is no good</td>
</tr>
<tr>
<td></td>
<td>clocking source from a trunk card or an external clock source.</td>
</tr>
</tbody>
</table>

**Command Default**

If no clocks are configured, the system uses a default, primary clock. An external clock is never selected by default; it must be explicitly configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The TDM bus can receive an input clock from one of three sources on the gateway:

- CT1, CE1, and CT3 trunk cards
- An external T1/E1 clock source feed directly through the Building Integrated Timing Supply (BITS) interface port on the motherboard
- Free-running clock providing clock from an oscillator

**Note**

BITS is a single building master timing supply. BITS generally supplies DS1- and DS0-level timing throughout an office. BITS is the clocks that provide and distribute timing to a wireline network’s lower levels.

**Trunk-Card Ports**

The TDM bus can be synchronized with any trunk cards. On the CT1/CE1 trunk card, each port receives the clock from the T1/E1 line. The CT3 trunk card uses an M13 multiplexer to receive the DS1 clock. Each port on each trunk-card slot has a default clock priority. Also, clock priority is configurable through the `tdm clock priority` command.

**External Clock**

The TDM bus can be synchronized with an external clock source that can be used as an additional network reference. If no clocks are configured, the system uses a primary clock through a software-controlled default
algorithm. If you want the external T1/E1 clock (from the BITS interface) as the primary clock source, you must configure it using the external keyword with the tdm clock priority command; the external clock is never selected by default.

The BITS interface requires a T1 line composite clock reference set at 1.544 MHz and an E1 line composite clock reference set at 2.048 MHz.

**Free-Running Clock**

If there is no good clocking source from a trunk card or an external clock source, then select the free-running clock from the internal oscillator using the freerun keyword with the tdm clock priority command.

**Examples**

In the following example, BITS clock is set at priority 1:

```
AS5400(config)# tdm clock priority priority 1 external
```

In the following example, a trunk clock from a CT1 trunk card is set at priority 2 and uses slot 4 and DS1 port (controller) 6:

```
AS5400(config)# tdm clock priority priority 2 4/6
```

In the following example, a trunk clock from a CT3 trunk card is set at priority 2 and uses slot 1, DS3 port 0, and DS1 port 19:

```
AS5400(config)# tdm clock priority priority 2 1/0:19
```

In the following example, free-running clock is set at priority 3:

```
AS5400(config)# tdm clock priority priority 3 freerun
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dial-tdm-clock</td>
<td>Configures the clock source and priority of the clock source used by the TDM bus on the dial shelf of the Cisco AS5800.</td>
</tr>
<tr>
<td>show tdm clocks</td>
<td>Displays default system clocks and clock history.</td>
</tr>
</tbody>
</table>

**terminal databits**

To change the number of data bits per character for the current terminal line for this session, use the terminal databits command in EXEC mode.

```
terminal databits {5|6|7|8}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Five data bits per character.</td>
</tr>
<tr>
<td>6</td>
<td>Six data bits per character.</td>
</tr>
<tr>
<td>7</td>
<td>Seven data bits per character.</td>
</tr>
<tr>
<td>8</td>
<td>Eight data bits per character. This is the default.</td>
</tr>
</tbody>
</table>
**Command Default**

8 data bits per character

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Communication protocols provided by devices such as terminals and modems often require a specific data bit setting. The `terminal databits` command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity generation is in effect, specify 8 data bits per character. The other keywords (5 and 6) are supplied for compatibility with older devices and are generally not used.

**Examples**

In the following example, the databits per character is changed to seven for the current session:

```
Router# terminal databits 7
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>databits</code></td>
<td>Sets the number of data bits per character that are interpreted and generated by the router hardware.</td>
</tr>
<tr>
<td><code>terminal parity</code></td>
<td>Defines the generation of the parity bit for the current terminal line and session.</td>
</tr>
</tbody>
</table>

**terminal data-character-bits**

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session, use the `terminal data-character-bits` command in EXEC mode.

```
terminal data-character-bits {7|8}
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Seven data bits per character.</td>
</tr>
<tr>
<td>8</td>
<td>Eight data bits. This is the default.</td>
</tr>
</tbody>
</table>

**Command Default**

8 data bits per character

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Cisco IOS Configuration Fundamentals Command Reference
Usage Guidelines

This command is used primarily to strip parity from X.25 connections on routers with the protocol translation software option. The terminal data-character-bits command does not work on hard-wired lines.

Examples

The following example sets the data bits per character to seven on the current line:

Router# terminal data-character-bits 7

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-character-bits</td>
<td>Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.</td>
</tr>
</tbody>
</table>

terminal dispatch-character

To define a character that causes a packet to be sent for the current session, use the terminal dispatch-character command in EXEC mode.

terminal dispatch-character [ascii-number [ascii-number2...]]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascii-number</td>
<td>The ASCII decimal representation of the character, such as Return (ASCII character 13) for line-at-a-time transmissions.</td>
</tr>
<tr>
<td>ascii-number2...</td>
<td>(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

At times, you might want to queue up a string of characters until they fill a complete packet and then transmit the packet to a remote host. This can make more efficient use of a line, because the access server or router normally dispatches each character as it is entered.

Examples

The following example defines the characters Ctrl-D (ASCII decimal character 4) and Ctrl-Y (ASCII decimal character 25) as the dispatch characters:

Router# terminal dispatch-character 4 25

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dispatch-character</td>
<td>Defines a character that causes a packet to be sent.</td>
</tr>
</tbody>
</table>
terminal dispatch-timeout

To set the character dispatch timer for the current terminal line for the current session, use the **terminal dispatch-timeout** command in EXEC mode.

**terminal dispatch-timeout milliseconds**

**Syntax Description**

| milliseconds | Integer that specifies the number of milliseconds that the router waits after it puts the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host. |

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to increase the processing efficiency of the remote host.

The **dispatch-timeout** line configuration command causes the software to buffer characters into packets for transmission to the remote host. The Cisco IOS software sends a packet a specified amount of time after the first character is put into the buffer. You can use the **terminal dispatch-timeout** and **terminal dispatch-character** line configuration commands together. In this case, the software dispatches a packet each time the dispatch character is entered, or after the specified dispatch timeout interval, depending on which condition is met first.

**Note**

The router response time might appear intermittent if the timeout interval is greater than 100 milliseconds and remote echoing is used.

**Examples**

In the following example, the dispatch timeout timer is set to 80 milliseconds:

```
Router# terminal dispatch-timeout 80
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dispatch-timeout</td>
<td>Sets the character dispatch timer for a specified line or group of lines.</td>
</tr>
</tbody>
</table>

terminal download

To temporarily set the ability of a line to act as a transparent pipe for file transfers for the current session, use the **terminal download** command in EXEC mode.

**terminal download**
This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use this feature to run a program such as KERMIT, XMODEM, or CrossTalk that downloads a file across an access server or router line. This command configures the terminal line to send data and is equivalent to entering all the following commands:

- `terminal telnet transparent`
- `terminal no escape-character` (see terminal escape-character)
- `terminal no hold-character` (see terminal hold-character)
- `terminal no padding 0` (see terminal padding)
- `terminal no padding 128` (see terminal padding)
- `terminal parity none`
- `terminal databits 8`

**Examples**

The following example configures a line to act as a transparent pipe:

```
Router# terminal download
```

---

**terminal editing**

To reenable the enhanced editing mode for only the current terminal session, use the `terminal editing` command in EXEC mode. To disable the enhanced editing mode on the current line, use the `no` form of this command.

```
terminal editing
terminal no editing
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Enabled

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command is identical to the editing EXEC mode command, except that it controls (enables or disables) enhanced editing for only the terminal session you are using. For a description of the available editing keys, see the description of the editing command in this document.

Examples

In the following example, enhanced editing mode is reenabled for only the current terminal session:

Router> terminal editing

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>editing</td>
<td>Controls CLI enhanced editing features for a particular line.</td>
</tr>
</tbody>
</table>

**terminal escape-character**

To set the escape character for the current terminal line for the current session, use the terminal escape-character command in EXEC mode.

terminal escape-character ascii-number

Syntax Description

| ascii-number | ASCII decimal representation of the escape character or control sequence (for example, Ctrl-P). |

Command Default

Ctrl-\^ (Ctrl-Shift-6)

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

See the "ASCII Character Set and Hexadecimal Values" appendix for a list of ASCII characters and their numerical representation.

This command is useful, for example, if you have the default escape character defined for a different purpose in your keyboard file. Entering the escape character followed by the X key returns you to EXEC mode when you are connected to another computer.

Note

The Break key generally cannot be used as an escape character on the console terminal because the operating software interprets the Break command on a console line as an instruction to halt the system.
Examples

In the following example, the escape character to Ctrl-P (ASCII decimal character 16) for the current session:

Router# terminal escape-character 16

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>escape-character</td>
<td>Defines a system escape character.</td>
</tr>
</tbody>
</table>

**terminal exec-character-bits**

To locally change the ASCII character set used in EXEC and configuration command characters for the current session, use the `terminal exec-character-bits` command in EXEC mode.

```
terminal exec-character-bits {7/8}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>7</th>
<th>Selects the 7-bit ASCII character set. This is the default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Selects the full 8-bit character set.</td>
</tr>
</tbody>
</table>

**Command Default**

7-bit ASCII character set (unless set otherwise in global configuration mode)

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This EXEC command overrides the `default-value exec-character-bits` global configuration command. Configuring the EXEC character width to 8 bits enables you to view special graphical and international characters in banners, prompts, and so on.

When the user exits the session, the character width is reset to the default value established by the `exec-character-bits` global configuration command. However, setting the EXEC character width to 8 bits can also cause failures. For example, if a user on a terminal that is sending parity enters the `help` command, an “unrecognized command” message appears because the system is reading all 8 bits, and the eighth bit is not needed for the `help` command.

**Examples**

The following example temporarily configures the system to use a full 8-bit user interface for system banners and prompts, allowing the use of additional graphical and international characters:

```
Router# terminal exec-character-bits 8
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exec-character-bits</td>
<td>Configures the character widths of EXEC and configuration command characters.</td>
</tr>
</tbody>
</table>

**terminal flowcontrol**

To set flow control for the current terminal line for the current session, use the `terminal flowcontrol` command in EXEC mode.

```
terminal flowcontrol {none|software[ {in|out} ]|hardware}
```

**Syntax Description**

- **none**: Prevents flow control.
- **software**: Sets software flow control.
- **in | out**: (Optional) Specifies the direction of flow control: *in* causes the router to listen to flow control from the attached device, and *out* causes the router to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
- **hardware**: Sets hardware flow control. For information about setting up the EIA/TIA-232 line, see the manual that was shipped with your product.

**Command Modes**

- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Flow control enables you to regulate the rate at which data can be transmitted from one point so that it is equal to the rate at which it can be received at another point. Flow control protects against loss of data because the terminal is not capable of receiving data at the rate it is being sent. You can set up data flow control for the current terminal line in one of two ways: software flow control, which you do with control key sequences, and hardware flow control, which you do at the device level.

For software flow control, the default stop and start characters are Ctrl-S and Ctrl-Q (XOFF and XON). You can change them with the `terminal stop-character` and `terminal start-character` EXEC commands.

**Examples**

In the following example, incoming software flow control is set for the current session:

```
Router# terminal flowcontrol software in
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flowcontrol</td>
<td>Sets the method of data flow control between the terminal or other serial device and the router.</td>
</tr>
</tbody>
</table>
terminal full-help

To get help for the full set of user-level commands, use the terminal full-help command in EXEC mode.

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The terminal full-help command enables a user to see all of the help messages available from the terminal. It is used with the show ? command.

Examples

In the following example, the difference between the output of the show ? command before and after using the terminal full-help command is shown:

Router> show ?
bootflash Boot Flash information
calendar Display the hardware calendar
clock Display the system clock
context Show context information
dialer Dialer parameters and statistics
history Display the session command history
hosts IP domain-name, lookup style, nameservers, and host table
isdn ISDN information
kerberos Show Kerberos Values
modemcap Show Modem Capabilities database
ppp PPP parameters and statistics
rmon rmon statistics
sessions Information about Telnet connections
snmp snmp statistics
terminal Display terminal configuration parameters
users Display information about terminal lines
version System hardware and software status

Router> terminal full-help
Router> show ?
access-expression List access expression
access-lists List access lists
aliases Display alias commands
apollo Apollo network information
apptalk AppleTalk information
arp ARP table
async Information on terminal lines used as router interfaces
bootflash Boot Flash information
bridge Bridge Forwarding/Filtering Database [verbose]
bsc BSC interface information
bstun BSTUN interface information
buffers | Buffer pool statistics
---|---
calendar | Display the hardware calendar
cdp | CDP information
clns | CLNS network information
clock | Display the system clock
cls | DLC user information
cmns | Connection-Mode networking services (CMNS) information
compress | Show compression statistics.
| .
| .
x25 | X.25 information
xns | XNS information
xremote | XRemote statistics

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full-help</td>
<td>Gets help for the full set of user-level commands.</td>
</tr>
<tr>
<td>help</td>
<td>Displays a brief description of the help system.</td>
</tr>
</tbody>
</table>

**terminal history**

To enable the command history function with 10 lines for the current terminal session, use the `terminal history` command in user EXEC or privileged EXEC mode. To disable the command history function, use the `no` form of this command.

```bash
terminal history
terminal no history
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Enabled, history buffer of 10 lines

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The history function provides a record of commands you have entered. This function is particularly useful for recalling long or complex commands or entries for the purposes of modifying them slightly and reexecuting them.

The `terminal history` command enables the command history function with the default buffer size or the last buffer size specified using the `terminal history size` command.

The following table lists the keys and functions you can use to recall commands from the history buffer.
**Table 180: History Keys**

<table>
<thead>
<tr>
<th>Key(s)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or Up Arrow</td>
<td>Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or Down Arrow</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
</tbody>
</table>

4 The arrow keys function only with ANSI-compatible terminals.

**Examples**

In the following example, the command history feature is disabled for the current terminal session:

```
Router> terminal no history
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>Enables the command history function, or changes the command history buffer size for a particular line.</td>
</tr>
<tr>
<td>show history</td>
<td>Lists the commands you have entered in the current EXEC session.</td>
</tr>
<tr>
<td>terminal history size</td>
<td>Sets the size of the history buffer for the command history feature for the current terminal session.</td>
</tr>
</tbody>
</table>

**terminal history size**

To change the size of the command history buffer for the current terminal session, use the `terminal history size` command in EXEC mode. To reset the command history buffer to its default size of 10 lines, use the `no` form of this command.

```
terminal history size number-of-lines
terminal no history size
```

**Syntax Description**

| number-of-lines | Number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10. |

**Command Default**

10 lines of command history

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The history feature provides a record of commands you have entered. This feature is particularly useful for recalling long or complex commands or entries for the purposes of modifying them slightly and reissuing them.

The `terminal history size` command enables the command history feature and sets the command history buffer size. The `terminal no history size` command resets the buffer size to the default of 10 command lines.

The following table lists the keys and functions you can use to recall commands from the history buffer. When you use these keys, the commands recalled will be from EXEC mode if you are in EXEC mode, or from all configuration modes if you are in any configuration mode.

<table>
<thead>
<tr>
<th>Key</th>
<th>Function</th>
</tr>
</thead>
</table>
| Ctrl-P or Up Arrow  
<sup>5</sup> | Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| Ctrl-N or Down Arrow  
<sup>1</sup> | Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands. |

<sup>5</sup> The arrow keys function only with ANSI-compatible terminals.

In EXEC mode, you can also use the `show history` command to show the contents of the command history buffer.

To check the current settings for the command history feature on your line, use the `show line` command.

Examples

In the following example, the number of command lines recorded is set to 15 for the current terminal session. The user then checks to see what line he/she is connected to using the `show users` command. The user uses this line information to issue the show line command. (In this example, the user uses the `show begin` option in the `show line` command to start the output at the “Editing is enabled/disabled” line.)

```
Router# terminal history size 15
Router# show users
Line Users Host(s) Idle Location
* 50 vty 0 admin idle 00:00:00
! the * symbol indicates the active terminal session for the user (line 50)
Router# show line 50 | begin Editing
Editing is enabled.
! the following line shows the history settings for the line
History is enabled, history size is 15.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are telnet. Preferred is none.
No output characters are padded
No special data dispatching characters
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>Enables the command history function, or changes the command history buffer size for a particular line.</td>
</tr>
</tbody>
</table>
terminal hold-character

To define the hold character for the current session, use the `terminal hold-character` command in EXEC mode. To return the hold character definition to the default, use the `no` form of this command.

```
terminal hold-character ascii-number
terminal no hold-character
```

**Syntax Description**
- `ascii-number`: ASCII decimal representation of a character or control sequence (for example, Ctrl-P).

**Command Default**
The default hold character is defined by the `hold-character` global configuration command.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You can define a local hold character that temporarily suspends the flow of output on the terminal. When information is scrolling too quickly, you can enter the hold character to pause the screen output, then enter any other character to resume the flow of output.

You cannot suspend output on the console terminal. To send the hold character to the host, precede it with the escape character.

**Examples**
In the following example, the hold character for the current (local) session is set to Ctrl-P. The `show terminal` output is included to show the verification of the setting (the value for the hold character is shown in the “Special Characters” listing).

```
Router# terminal hold-character 16
"^P" is the local hold character
Router# show terminal
Line 50, Location: ", Type: "VT220"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: PSI Enabled, Ready, Active, No Exit Banner, Automore On
Capabilities: none
Modem state: Ready
Group codes: 0
Special Chars: Escape Hold Stop Start Disconnect Activation
```
Modem type is unknown.
Session limit is not set.
Time since activation: 00:04:13
Editing is enabled.
History is enabled, history size is 10.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hold-character</strong></td>
<td>Defines the local hold character used to pause output to the terminal screen.</td>
</tr>
<tr>
<td><strong>show terminal</strong></td>
<td>Displays settings for terminal operating characteristics.</td>
</tr>
</tbody>
</table>

**terminal international**

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[] for a current Telnet session, use the `terminal international` command in user EXEC or privileged mode. To display characters in 7-bit format for a current Telnet session, use the `no` form of this command.

```
terminal international
no terminal international
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

User EXEC
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you are configuring a Cisco IOS platform using the Cisco web browser UI, this feature is enabled automatically when you enable the Cisco web browser UI using the `ip http server` global configuration command.


Examples

The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[) when you are using Telnet to access the platform for the current Telnet session:

Router# terminal international

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>international</td>
<td>Prints the Escape character as a single character instead of as the caret and bracket symbols (^[) in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).</td>
</tr>
</tbody>
</table>

terminal keymap-type

To specify the current keyboard type for the current session, use the terminal keymap-type command in EXEC mode.

terminal keymap-type keymap-name

Syntax Description

| keymap-name | Name defining the current keyboard type. |

Command Default

VT100

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You must use this command when you are using a keyboard other than the default of VT100.

Examples

The following example specifies a VT220 keyboard as the current keyboard type:

Router# terminal keymap-type vt220

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show keymap</td>
<td>Displays the current keymap settings.</td>
</tr>
</tbody>
</table>

terminal length

To set the number of lines on the current terminal screen for the current session, use the terminal length command in EXEC, privileged EXEC, and diagnostic mode.
**terminal length** `screen-length`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th><code>screen-length</code> Number of lines on the screen. A value of zero disables pausing between screens of output.</th>
</tr>
</thead>
</table>

**Command Default**  
24 lines

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers, and became available in diagnostic mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  
The system uses the length value to determine when to pause during multiple-screen output. A value of zero prevents the router from pausing between screens of output.

Some types of terminal sessions do not require you to specify the screen length because the screen length specified can be learned by some remote hosts. For example, the rlogin protocol uses the screen length to set up terminal parameters on a remote UNIX host.

**Examples**  
In the following example, the system is configured to prevent output from pausing if it exceeds the length of the screen:

Router# `terminal length 0`

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>Sets the terminal screen length.</td>
</tr>
</tbody>
</table>

**terminal monitor**

To display `debug` command output and system error messages for the current terminal and session, use the `terminal monitor` command in EXEC mode.

```
terminal monitor
```

**Syntax Description**  
This command has no arguments or keywords.

**Command Default**  
Disabled

**Command Modes**  
EXEC
terminal notify

To enable terminal notification about pending output from other Telnet connections for the current session, use the terminal notify command in EXEC mode. To disable notifications for the current session, use the no form of this command.

```
terminal notify
terminal no notify
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Usage Guidelines**

Enabling notifications may be useful if, for example, you want to know when another connection receives mail, or when a process has been completed.

This command enables or disables notifications for only the current session. To globally set these notifications, use the notify line configuration command.

**Examples**

In the following example, notifications will be displayed to inform the user when output is pending on another connection:

```
Router# terminal notify
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notify</td>
<td>Enables terminal notification about pending output from other Telnet connections.</td>
</tr>
</tbody>
</table>
terminal padding

To change the character padding on a specific output character for the current session, use the `terminal padding` command in EXEC mode.

`terminal padding ascii-number count`

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascii-number</td>
<td>ASCII decimal representation of the character.</td>
</tr>
<tr>
<td>count</td>
<td>Number of NULL bytes sent after the specified character, up to 255 padding characters in length.</td>
</tr>
</tbody>
</table>

Command Default

No padding

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Character padding adds a number of null bytes to the end of the string and can be used to make a string an expected length for conformity.

Use this command when the attached device is an old terminal that requires padding after certain characters (such as ones that scrolled or moved the carriage). See the "ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters.

Examples

The following example pads Ctrl-D (ASCII decimal character 4) with 164 NULL bytes:

```
Router# terminal padding 4 164
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>padding</td>
<td>Sets the padding on a specific output character.</td>
</tr>
</tbody>
</table>

terminal parity

To define the generation of the parity bit for the current terminal line and session, use the `terminal parity` command in EXEC mode.

`terminal parity {none|even|odd|space|mark}`

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No parity. This is the default.</td>
</tr>
<tr>
<td>even</td>
<td>Even parity.</td>
</tr>
</tbody>
</table>
### terminal rxspeed

To set the terminal receive speed (how fast information is sent to the terminal) for the current line and session, use the `terminal rxspeed` command in EXEC mode.

#### Syntax

```
terminal rxspeed bps
```

#### Syntax Description

- **bps**: Baud rate in bits per second (bps). The default is 9600.

#### Command Default

- **9600 bps**

#### Command Modes

- **EXEC**

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

---

### terminal parity

<table>
<thead>
<tr>
<th>odd</th>
<th>Odd parity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>space</td>
<td>Space parity.</td>
</tr>
<tr>
<td>mark</td>
<td>Mark parity.</td>
</tr>
</tbody>
</table>

#### Command Default

- **No parity.**

#### Command Modes

- **EXEC**

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Communication protocols provided by devices such as terminals and modems will sometimes require a specific parity bit setting. Refer to the documentation for your device to determine required parity settings.

#### Examples

In the following example, odd parity checking is enabled for the current session:

```
Router# terminal parity odd
```
Usage Guidelines

Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the system. The system will indicate if the speed you select is not supported.

Examples

The following example sets the current auxiliary line receive speed to 115200 bps:

Router# terminal rxspeed 115200

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rxspeed</td>
<td>Sets the terminal receive speed for a specified line or lines.</td>
</tr>
<tr>
<td>terminal rxspeed</td>
<td>Sets the terminal receive speed for the current session.</td>
</tr>
<tr>
<td>terminal txspeed</td>
<td>Sets the terminal transmit speed for a specified line or lines.</td>
</tr>
<tr>
<td>terminal speed</td>
<td>Sets the transmit and receive speeds for the current session.</td>
</tr>
</tbody>
</table>

terminal special-character-bits

To change the ASCII character widths to accept special characters for the current terminal line and session, use the terminal special-character-bits command in EXEC mode.

```
terminal special-character-bits
```

7/8

Syntax Description

<table>
<thead>
<tr>
<th>7</th>
<th>Selects the 7-bit ASCII character set. This is the default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Selects the full 8-bit ASCII character set.</td>
</tr>
</tbody>
</table>

Command Default

7-bit ASCII character set

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Configuring the width to 8 bits enables you to use twice as many special characters as with the 7-bit setting. This selection enables you to add special graphical and international characters in banners, prompts, and so on.

This command is useful, for example, if you want the router to provide temporary support for international character sets. It overrides the default-value special-character-bits global configuration command and is used to compare character sets typed by the user with the special character available during a data connection, which includes software flow control and escape characters.
When you exit the session, character width is reset to the width established by the `default-value exec-character-bits` global configuration command.

Note that setting the EXEC character width to eight bits can cause failures. For example, if a user on a terminal that is sending parity enters the `help` command, an “unrecognized command” message appears because the Cisco IOS software is reading all eight bits, and the eighth bit is not needed for the `help` command.

### Examples

The following example temporarily configures a router to use a full 8-bit user interface for system banners and prompts.

```
Router# terminal special-character-bits 8
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-value exec-character-bits</code></td>
<td>Globally defines the character width as 7-bit or 8-bit.</td>
</tr>
<tr>
<td><code>special-character-bits</code></td>
<td>Configures the number of data bits per character for special characters such as software flow control characters and escape characters.</td>
</tr>
</tbody>
</table>

### terminal speed

To set the transmit and receive speeds of the current terminal line for the current session, use the `terminal speed` command in EXEC mode.

```
terminal speed bps
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bps</code></td>
<td>Baud rate in bits per second (bps). The default is 9600.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>9600 bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Set the speed to match the transmission rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the router. The router indicates whether the speed you selected is not supported.

### Examples

The following example restores the transmit and receive speed on the current line to 9600 bps:

```
Router# terminal speed 9600
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>speed</td>
<td>Sets the terminal baud rate.</td>
</tr>
</tbody>
</table>

**terminal start-character**

To change the flow control start character for the current session, use the `terminal start-character` command in EXEC mode.

```
terminal start-character ascii-number
```

**Syntax Description**

- `ascii-number`: ASCII decimal representation of the start character.

**Command Default**

Ctrl-Q (ASCII decimal character 17)

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The flow control start character signals the start of data transmission when software flow control is in effect.

**Examples**

The following example changes the start character to Ctrl-O (ASCII decimal character 15):

```
Router# terminal start-character 15
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-character</td>
<td>Sets the flow control start character.</td>
</tr>
</tbody>
</table>

**terminal stopbits**

To change the number of stop bits sent per byte by the current terminal line during an active session, use the `terminal stopbits` command in EXEC mode.

```
terminal stopbits {1|1.5|2}
```

**Syntax Description**

- 1: One stop bit.
- 1.5: One and one-half stop bits.
- 2: Two stop bits. This is the default.
terminal stop-character

Command Default
2 stop bits

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.

Examples
In the following example, the setting for stop bits is changed to one for the current session:

```
Router# terminal stopbits 1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stopbits</td>
<td>Sets the number of the stop bits sent per byte.</td>
</tr>
</tbody>
</table>

**terminal stop-character**

To change the flow control stop character for the current session, use the `terminal stop-character` command in EXEC mode.

```
terminal stop-character ascii-number
```

Syntax Description

| ascii-number | ASCII decimal representation of the stop character. |

Command Default
Ctrl-S (ASCII character decimal 19)

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The flow control stop character signals the end of data transmission when software flow control is in effect. See the "ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters.

Examples
In the following example, the stop character is configured as Ctrl-E (ASCII character decimal 5) for the current session:

```
```
Router# terminal stop-character 5

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stop-character</td>
<td>Sets the flow control stop character.</td>
</tr>
</tbody>
</table>

## terminal telnet break-on-ip

To cause an access server to generate a hardware Break signal when an interrupt-process (ip) command is received, use the terminal telnet break-on-ip command in EXEC mode.

### Syntax Description

This command has no arguments or keywords.

### Command Default

Disabled

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The hardware Break signal occurs when a Telnet interrupt-process (ip) command is received on that connection. The terminal telnet break-on-ip command can be used to control the translation of Telnet interrupt-process commands into X.25 Break indications.

Note

In this command, the acronym “ip” indicates “interrupt-process,” not Internet Protocol (IP).

This command is also a useful workaround in the following situations:

- Several user Telnet programs send an ip command, but cannot send a Telnet Break signal.
- Some Telnet programs implement a Break signal that sends an ip command.

Some EIA/TIA-232 hardware devices use a hardware Break signal for various purposes. A hardware Break signal is generated when a Telnet Break command is received.

You can verify if this command is enabled with the show terminal EXEC command. If enabled the following line will appear in the output: Capabilities: Send BREAK on IP.

### Examples

In the following example, a Break signal is generated for the current connection when an interrupt-process command is issued:

Router# terminal telnet break-on-ip
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal telnet ip-on-break</td>
<td>Configures the system to send an interrupt-process (ip) signal when the Break command is issued.</td>
</tr>
</tbody>
</table>

**terminal telnet refuse-negotiations**

To configure the current session to refuse to negotiate full-duplex, remote echo options on incoming connections, use the `terminal telnet refuse-negotiations` command in EXEC mode.

**terminal telnet refuse-negotiations**

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Disabled

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You can set the line to allow access server to refuse full-duplex, remote echo connection requests from the other end. This command suppresses negotiation of the Telnet Remote Echo and Suppress Go Ahead options.

**Examples**

In the following example, the current session is configured to refuse full-duplex, remote echo requests:

```
Router# terminal telnet refuse-negotiations
```

**terminal telnet speed**

To allow an access server to negotiate transmission speed for the current terminal line and session, use the `terminal telnet speed` command in EXEC mode.

**terminal telnet speed default-speed maximum-speed**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-speed</td>
<td>Line speed, in bits per second (bps), that the access server will use if the device on the other end of the connection has not specified a speed.</td>
</tr>
<tr>
<td>maximum-speed</td>
<td>Maximum line speed in bits per second (bps), that the device on the other end of the connection can use.</td>
</tr>
</tbody>
</table>

**Command Default**
9600 bps (unless otherwise set using the `speed`, `txspeed` or `rxspeed` line configuration commands)

**Command Modes**
EXEC
This command was introduced."},
10.0: This command was introduced.
12.2(33)SRA: This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can match line speeds on remote systems in reverse Telnet, on host machines connected to an access server to access the network, or on a group of console lines connected to the access server when disparate line speeds are in use at the local and remote ends of the connections listed above. Line speed negotiation adheres to the Remote Flow Control option, defined in RFC 1080.

Note

This command applies only to access servers. It is not supported on standalone routers.

Examples

The following example enables the access server to negotiate a bit rate on the line using the Telnet option. If no speed is negotiated, the line will run at 2400 bps. If the remote host requests a speed greater than 9600 bps, then 9600 bps will be used.

Router# terminal telnet speed 2400 9600

terminal telnet sync-on-break

To cause the access server to send a Telnet Synchronize signal when it receives a Telnet Break signal on the current line and session, use the terminal telnet sync-on-break command in EXEC mode.

terminal telnet sync-on-break

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can configure the session to cause a reverse Telnet line to send a Telnet Synchronize signal when it receives a Telnet Break signal. The TCP Synchronize signal clears the data path, but still interprets incoming commands.

Note

This command applies only to access servers. It is not supported on standalone routers.
Examples

The following example sets an asynchronous line to cause the access server to send a Telnet Synchronize signal:

```plaintext
Router# terminal telnet sync-on-break
```

terminal telnet transparent

To cause the current terminal line to send a Return character (CR) as a CR followed by a NULL instead of a CR followed by a Line Feed (LF) for the current session, use the `terminal telnet transparent` command in EXEC mode.

```plaintext
terminal telnet transparent
```

Syntax Description

This command has no arguments or keywords.

Command Default

CR followed by an LF

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The end of each line typed at the terminal is ended with a Return (CR). This command permits interoperability with different interpretations of end-of-line demarcation in the Telnet protocol specification.

Note

This command applies only to access servers. It is not supported on stand-alone routers.

Examples

In the following example, the session is configured to send a CR signal as a CR followed by a NULL:

```plaintext
Router# terminal telnet transparent
```

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the `terminal terminal-type` command in EXEC, privileged EXEC, and diagnostic mode.

```plaintext
terminal terminal-type  terminal-type
```

Syntax Description

<table>
<thead>
<tr>
<th>terminal-type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal-type</td>
<td>Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. The default is VT100.</td>
</tr>
</tbody>
</table>
VT100

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers, and became available in diagnostic mode.</td>
</tr>
</tbody>
</table>

Indicate the terminal type if it is different from the default of VT100.

The terminal type name is used by TN3270s for display management and by Telnet and rlogin to inform the remote host of the terminal type.

In the following example, the terminal type is defined as VT220 for the current session:

```
Router# terminal terminal-type VT220
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal keymap-type</td>
<td>Specifies the current keyboard type for the current session.</td>
</tr>
<tr>
<td>terminal-type</td>
<td>Specifies the type of terminal connected to a line.</td>
</tr>
</tbody>
</table>

**terminal txspeed**

To set the terminal transmit speed (how fast the terminal can send information) for the current line and session, use the `terminal txspeed` command in EXEC mode.

```
terminal txspeed bps
```

**Syntax Description**

| bps | Baud rate in bits per second (bps). The default is 9600 bps. |

**Command Default**

9600 bps

**Command Modes**

EXEC

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
In the following example, the line transmit speed is set to 2400 bps for the current session:

```
Router# terminal txspeed 2400
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rxspeed</td>
<td>Sets the terminal receive speed for a specified line or lines.</td>
</tr>
<tr>
<td>terminal rxspeed</td>
<td>Sets the terminal receive speed for the current line and session.</td>
</tr>
<tr>
<td>terminal terminal-type</td>
<td>Specifies the type of terminal connected to the current line for the current session.</td>
</tr>
<tr>
<td>txspeed</td>
<td>Sets the terminal transmit speed for a specified line or lines.</td>
</tr>
</tbody>
</table>

**terminal width**

To set the number of character columns on the terminal screen for the current line for a session, use the `terminal width` command in EXEC, privileged EXEC, or diagnostic mode.

```
terminal width characters
```

**Syntax Description**

- **characters**: Number of character columns displayed on the terminal. The default is 80 characters.

**Command Default**

80 characters

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on the Cisco ASR 1000 Series Routers, and became available in diagnostic mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal.

The rlogin protocol uses the value of the `characters` argument to set up terminal parameters on a remote host.

**Examples**

The following example sets the terminal character columns to 132:

```
Router# terminal width 132
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>width</td>
<td>Sets the terminal screen width (the number of character columns displayed on the attached terminal).</td>
</tr>
</tbody>
</table>

**terminal-queue entry-retry-interval**

To change the retry interval for a terminal port queue, use the `terminal-queue entry-retry-interval` command in global configuration mode. To restore the default terminal port queue interval, use the `no` form of this command.

```
terminal-queue entry-retry-interval seconds
no terminal-queue entry-retry-interval
```

**Syntax Description**

| seconds   | Number of seconds between terminal port retries. The default is 60 seconds. |

**Command Default**

60 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If a remote device (such as a printer) is busy, the connection attempt is placed in a terminal port queue. If you want to decrease the waiting period between subsequent connection attempts, decrease the default of 60 to an interval of 10 seconds. Decrease the time between subsequent connection attempts when, for example, a printer queue stalls for long periods.

**Examples**

The following example changes the terminal port queue retry interval from the default of 60 seconds to 10 seconds:

```
Router# terminal-queue entry-retry-interval 10
```

**terminal-type**

To specify the type of terminal connected to a line, use the `terminal-type` command in line configuration mode. To remove any information about the type of terminal and reset the line to the default terminal emulation, use the `no` form of this command.

```
terminal-type {terminal-name terminal-type}
no terminal-type
```

**Syntax Description**

| terminal-name | Terminal name.                                      |
terminal-type

<table>
<thead>
<tr>
<th>terminal-type</th>
<th>Terminal type</th>
</tr>
</thead>
</table>

**Command Default**
VT100

**Command Modes**
Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command records the type of terminal connected to the line. The `terminal-name` argument provides a record of the terminal type and allows terminal negotiation of display management by hosts that provide that type of service.

For TN3270 applications, this command must follow the corresponding `ttycap` entry in the configuration file.

**Examples**
The following example defines the terminal on line 7 as a VT220:

```
Router(config)# line 7
Router(config-line)# terminal-type VT220
```
test cable-diagnostics through xmodem

- test cable-diagnostics through xmodem, on page 1058
test cable-diagnostics through xmodem

**test cable-diagnostics**

To test the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules, use the test cable-diagnostics command in privileged EXEC mode.

```bash
test cable-diagnostics tdr interface type number
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tdr</td>
<td>Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.</td>
</tr>
<tr>
<td>interface type</td>
<td>Specifies the interface type; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>number</td>
<td>Module and port number.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17a)SX</td>
<td>Support for this command was introduced on the Cisco 7600 series routers.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was changed to provide support for the 4-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6704-10GE).</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Cable diagnostics can help you detect whether your cable has connectivity problems.

The TDR test guidelines are as follows:

- TDR can test cables up to a maximum length of 115 meters.
- The TDR test is supported on Cisco 7600 series routers running Release 12.2(17a)SX and later releases on specific modules. See the Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2 for the list of the modules that support TDR.
- The valid values for interface type are fastethernet and gigabitethernet.
- Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.
- Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.
• The interface must be up before running the TDR test. If the port is down, the `test cable-diagnostics tdr` command is rejected and the following message is displayed:

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

• If the port speed is 1000 and the link is up, do not disable the auto-MDIX feature.

• For fixed 10/100 ports, before running the TDR test, disable auto-MDIX on both sides of the cable. Failure to do so can lead to misleading results.

• For all other conditions, you must disable the auto-MDIX feature on both ends of the cable (use the `no mdix auto` command). Failure to disable auto-MDIX will interfere with the TDR test and generate false results.

• If a link partner has auto-MDIX enabled, this action will interfere with the TDR-cable diagnostics test and test results will be misleading. The workaround is to disable auto-MDIX on the link partner.

• If you change the port speed from 1000 to 10/100, enter the `no mdix auto` command before running the TDR test. Note that entering the `speed 1000` command enables auto-MDIX regardless of whether the `no mdix auto` command has been run.

**Examples**

This example shows how to run the TDR-cable diagnostics:

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cable-diag tdr</td>
<td>Clears a specific interface or clears all interfaces that support TDR.</td>
</tr>
<tr>
<td>show cable-diag tdr</td>
<td>Displays the test results for the TDR cable diagnostics.</td>
</tr>
</tbody>
</table>

**test flash**

To test Flash memory on MCI and envm Flash EPROM interfaces, use the `test flash` command in EXEC mode.

```
  test flash
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command has no default values.

**Command Modes**

EXEC
test interfaces

To test the system interfaces on the modular router, use the test interfaces command in EXEC mode.

test interfaces

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
This command has no default values.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The test interfaces EXEC command is intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router. The test interfaces output does not report correct results if the router is attached to a “live” network. For each network interface that has an IP address that can be tested in loopback (MCI and ciscoBus Ethernet and all serial interfaces), the test interfaces command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

**Examples**

In the following example, the system interfaces are tested:

test interfaces

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test flash</td>
<td>Tests Flash memory on MCI and envm Flash EPROM interfaces.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the Flash memory is tested:

test flash
**test memory**

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the `test memory` command in privileged EXEC mode. The memory test overwrites memory.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command overwrites memory.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The memory test overwrites memory. If you use the `test memory` command, you will need to rewrite nonvolatile memory. For example, if you test Multibus memory, which is the memory used by the CSC-R 4-Mbps Token Ring interfaces, you will need to reload the system before the network interfaces will operate properly. The `test memory` command is intended primarily for use by Cisco personnel.

**Examples**

In the following example, the memory is tested:

```
test memory
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test flash</td>
<td>Tests Flash memory on MCI and envm Flash EPROM interfaces.</td>
</tr>
<tr>
<td>test interfaces</td>
<td>Tests the system interfaces on the modular router.</td>
</tr>
</tbody>
</table>

**test memory destroy**

To destroy a memory chunk or dangling reference, use the `test memory destroy` command in privileged EXEC mode.

```
test memory destroy [{chunk|mgd-chunk|force-chunk|dangling-reference}] chunk-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>chunk</th>
<th>(Optional) Ordinary chunk of memory.</th>
</tr>
</thead>
</table>

---

**Cisco IOS Configuration Fundamentals Command Reference**

---
### test platform police get

To get the IPv6 internal police rate, use the `test platform police get` command in privileged EXEC mode.

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

0 (No rate has been applied.)

#### Command Modes

Privileged EXEC (#)
The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

### Usage Guidelines

Use this command under the `exec` command of the line card console. It is not visible from the route processor (RP) console.

### Examples

The following example shows how to get the IPv6 internal police rate:

```plaintext
Router> enable
Router# test platform police get
IPv6 with HBH header is policed at 100000 kbps
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>test platform police set</strong></td>
<td>Sets the IPv6 internal police rate.</td>
</tr>
</tbody>
</table>

### test platform police set

To set the IPv6 internal police rate, use the **test platform police set** command in privileged EXEC mode.

This command does not have a no form.

```plaintext
test platform police set rate
```

### Syntax Description

- **rate**
  - Specifies the internal police rate. The range is from 0 to 100000 kbps.
  - For the SIP-400, you can configure a rate up to, and including 25600 packets per second (PPS).
  - For the ES+ line cards and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG line cards, you can configure rates of:
    - 16 Kbps to 2 Mbps; granularity of 16 kbps
    - 2 Mbps to 100 Mbps; granularity of 64 kbps

### Command Default

For ES40 line cards, the default police rate is 12.8 Mbps.
For the SIP-400, the default police rate is 21.36 kpps.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRD1</td>
<td>The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command under the EXEC command of the line card console. It is not visible from the route processor (RP) console.
There is not a **no** version of this command. If you have set a rate limit and wish to cancel it, you will need to use this command to set the rate to 0.

For both the ES+ line cards and the SIP-400, setting the police rate to 0 turns off the policing.

For both the ES+ line cards and the SIP-400, when the policer is set from the the line card console, the setting remains effective even if the line card is moved to another chassis running the Cisco IOS Release 12.2(33)SRD1 (or later) image.

For the SIP-400, IPv6 HBH packets will continue to go through the QoS policing configured on the line card. For ES+ line cards, IPv6 HBH packets will bypass any QoS configured on the line card.

**Examples**

The following examples shows how to set the IPv6 with HBH header to be policed at 100000 kbps:

```plaintext
Router> enable
Router# test platform police set 100000
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>test platform police get</td>
<td>Gets the IPv6 internal police rate.</td>
</tr>
</tbody>
</table>

**tftp-server**

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** commands in global configuration mode. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename.

```plaintext
tftp-server flash [partition-number :] filename1 [alias filename2] [access-list-number]
tftp-server rom alias filename1 [access-list-number]
no tftp-server {flash [partition-number :] filename1|rom alias filename2}
```

**Cisco 1600 Series and Cisco 3600 Series Routers**

```plaintext
tftp-server flash [device :] [partition-number :] filename
no tftp-server flash [device :] [partition-number :] filename
```

**Cisco 7000 Family Routers**

```plaintext
tftp-server flash device : filename
no tftp-server flash device : filename
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>flash</th>
<th>rom</th>
<th>filename1</th>
<th>alias</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specifies TFTP service of a file in Flash memory.</td>
<td>Specifies TFTP service of a file in ROM.</td>
<td>Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.</td>
<td>Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.</td>
</tr>
</tbody>
</table>
### filename2
Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.

<table>
<thead>
<tr>
<th>access-list-number</th>
<th>(Optional) Basic IP access list number. Valid values are from 0 to 99.</th>
</tr>
</thead>
<tbody>
<tr>
<td>partition-number</td>
<td>(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used. For the Cisco 1600 series and Cisco 3600 series routers, you must enter a colon after the partition number if a filename follows it.</td>
</tr>
</tbody>
</table>
| device             | (Optional) Specifies TFTP service of a file on a Flash memory device in the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers. The colon is required. Valid devices are as follows:  
  - **flash** --Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. This is the only valid device for the Cisco 1600 series routers.  
  - **bootflash** --Internal Flash memory in the Cisco 7000 family routers.  
  - **slot0** --First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers.  
  - **slot1** --Second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family.  
  - **slavebootflash** --Internal Flash memory on the slave RSP card of a Cisco 7507 or Cisco 7513 router configured for HSA.  
  - **slaveslot0** --First PCMCIA slot on the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.  
  - **slaveslot1** --Second PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA. |

| filename            | Name of the file on a Flash memory device that the TFTP server uses in answering a TFTP Read Request. Use this argument only with the Cisco 1600 series, Cisco 3600 series, Cisco 7000 series, or Cisco 7500 series routers. |

### Command Default
Disabled

### Command Modes
Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
You can specify multiple filenames by repeating the `tftp-server` command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any client that issues a TFTP Read Request with this filename.
If the specified `filename1` or `filename2` argument exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified `filename1` or `filename2` argument is not found in Flash memory.

Images that run from ROM cannot be loaded over the network. Therefore, it does not make sense to use TFTP to offer the ROMs on these images.

On the Cisco 7000 family routers, the system sends a copy of the file contained on one of the Flash memory devices to any client that issues a TFTP Read Request with its filename.

**Examples**

In the following example, the system uses TFTP to send a copy of the `version-10.3` file located in Flash memory in response to a TFTP Read Request for that file. The requesting host is checked against access list 22.

```
tftp-server flash version-10.3 22
```

In the following example, the system uses TFTP to send a copy of the ROM image `gs3-k.101` in response to a TFTP Read Request for the `gs3-k.101` file:

```
tftp-server rom alias gs3-k.101
```

In the following example, the system uses TFTP to send a copy of the `version-11.0` file in response to a TFTP Read Request for that file. The file is located on the Flash memory card inserted in slot 0.

```
tftp-server flash slot0:version-11.0
```

The following example enables a Cisco 3600 series router to operate as a TFTP server. The source file `c3640-i-mz` is in the second partition of internal Flash memory.

```
Router#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c3640-i-mz
```

In the following example, the source file is in the second partition of the Flash memory PC card in slot 0 on a Cisco 3600 series:

```
Router#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# tftp-server flash slot0:2:dirt/gate/c3640-j-mz
```

The following example enables a Cisco 1600 series router to operate as a TFTP server. The source file `c1600-i-mz` is in the second partition of Flash memory:

```
router#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c1600-i-mz
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list</code></td>
<td>Creates an extended access list.</td>
</tr>
</tbody>
</table>
tftp-server system

The `tftp-server system` command has been replaced by the `tftp-server` command. See the description of the tftp-server command in this chapter for more information.

**time-period**

To set the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive, use the `time-period` command in archive configuration mode. To disable this function, use the `no` form of this command.

```
time-period  minutes
no  time-period  minutes
```

**Syntax Description**

| minutes | Specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco configuration archive. |

**Command Default**

No time increment is set.

**Command Modes**

Archive configuration (config-archive)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB</td>
<td>This command was implemented on the Cisco 10000 series router.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

Before using this command, you must configure the `path` command to specify the location and filename prefix for the files in the Cisco configuration archive.

If this command is configured, an archive file of the current running configuration is automatically saved after the given time specified by the `minutes` argument. Archive files continue to be automatically saved at this
given time increment until this function is disabled. Use the `maximum` command to set the maximum number of archive files of the running configuration to be saved.

**Note**
This command saves the current running configuration to the configuration archive whether or not the running configuration has been modified since the last archive file was saved.

**Examples**
In the following example, a value of 20 minutes is set as the time increment for which to automatically save an archive file of the current running configuration in the Cisco configuration archive:

```
Device# configure terminal
Device(config)# archive
Device(config-archive)# path disk0:myconfig
Device(config-archive)# time-period 20
Device(config-archive)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>archive</code></td>
<td>Saves a copy of the current running configuration to the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>configure confirm</code></td>
<td>Confirms replacement of the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td><code>configure replace</code></td>
<td>Replaces the current running configuration with a saved Cisco configuration file.</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>path</code></td>
<td>Specifies the location and filename prefix for the files in the Cisco configuration archive.</td>
</tr>
<tr>
<td><code>show archive</code></td>
<td>Displays information about the files saved in the Cisco configuration archive.</td>
</tr>
</tbody>
</table>

---

### trace (privileged)

To discover the routes that packets will actually take when traveling to their destination, use the `trace` command in privileged EXEC mode.

```
trace [protocol] [destination]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>(Optional) Protocols that can be used are <code>appletalk</code>, <code>clns</code>, <code>ip</code> and <code>vines</code>.</td>
</tr>
<tr>
<td>destination</td>
<td>(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.</td>
</tr>
</tbody>
</table>

**Command Default**

The `protocol` argument is based on the Cisco IOS software examination of the format of the `destination` argument. For example, if the software finds a `destination` argument in IP format, the `protocol` value defaults to `ip`. 
The `trace` command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The `trace` command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The `trace` command sends several probes at each TTL level and displays the round-trip time for each.

The `trace` command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the `trace` command prints an asterisk (*).

The `trace` command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type Ctrl-^X by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

To use nondefault parameters and invoke an extended `trace` test, enter the command without a `destination` argument. You will be stepped through a dialog to select the desired parameters.

**Common Trace Problems**

Due to bugs in the IP implementation of various hosts and routers, the IP `trace` command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message but they reuse the TTL of the incoming packet. Because this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the ICMP message can get back. For example, if the host is six hops away, the `trace` command will time out on responses 6 through 11.

**Trace IP Routes**

The following display shows sample IP `trace` output when a destination host name has been specified:

```bash
Router# trace ABA.NYC.mil
Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
  1 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
  2 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
  3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
```
The following table describes the significant fields shown in the display.

### Table 182: trace Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates the sequence number of the router in the path to the host.</td>
</tr>
<tr>
<td>DEBRIS.CISCO.COM</td>
<td>Host name of this router.</td>
</tr>
<tr>
<td>192.180.1.6</td>
<td>Internet address of this router.</td>
</tr>
<tr>
<td>1000 msec 8 msec 4 msec</td>
<td>Round-trip time for each of the three probes that are sent.</td>
</tr>
</tbody>
</table>

### Extended IP Trace Dialog

The following display shows a sample `trace` session involving the extended dialog of the `trace` command:

```
Router# trace
Protocol [ip]:
Target IP address: mit.edu
Source address: numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Type escape sequence to abort.
Tracing the route to MIT.EDU (18.72.2.1)
 1 ICMP-DC-2-V1.ICP.NET (192.108.209.17) 72 msec 72 msec 88 msec
 2 ICMP-FIX-E-H0-T3.ICP.NET (192.157.65.122) 80 msec 128 msec 80 msec
 3 192.203.229.246 540 msec 88 msec 84 msec
 4 T3-2.WASHINGTON-DC-CNSS58.T3.ANS.NET (140.222.58.3) 84 msec 116 msec 88 msec
 5 T3-3.WASHINGTON-DC-CNSS56.T3.ANS.NET (140.222.56.4) 80 msec 132 msec 88 msec
 6 T3-0.NEW-YORK-CNSS32.T3.ANS.NET (140.222.32.1) 92 msec 132 msec 88 msec
 7 T3-0.HARTFORD-CNSS48.T3.ANS.NET (140.222.48.1) 88 msec 88 msec 88 msec
 8 T3-0.HARTFORD-CNSS49.T3.ANS.NET (140.222.49.1) 96 msec 104 msec 96 msec
 9 T3-0.ENSS134.T3.ANS.NET (140.222.134.1) 92 msec 128 msec 92 msec
10 W91-CISCO-EXTERNAL-FDDI.MIT.EDU (192.233.33.1) 92 msec 92 msec 112 msec
11 E40-RTR-FDDI.MIT.EDU (18.168.0.2) 92 msec 120 msec 96 msec
12 MIT.EDU (18.72.2.1) 96 msec 92 msec 96 msec
```

The following table describes the fields that are unique to the extended trace sequence, as shown in the display.

### Table 183: trace Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target IP address</td>
<td>You must enter a host name or an IP address. There is no default.</td>
</tr>
<tr>
<td>Source address</td>
<td>One of the interface addresses of the router to use as a source address for the probes. The router will normally pick what it feels is the best source address to use.</td>
</tr>
</tbody>
</table>
The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.

### Timeout in seconds
The number of seconds to wait for a response to a probe packet. The default is 3 seconds.

### Probe count
The number of probes to be sent at each TTL level. The default count is 3.

### Minimum Time to Live [1]
The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.

### Maximum Time to Live [30]
The largest TTL value that can be used. The default is 30. The `trace` command terminates when the destination is reached or when this value is reached.

### Port Number
The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.

### Loose, Strict, Record, Timestamp, Verbose
IP header options. You can specify any combination. The `trace` command issues prompts for the required fields. Note that the `trace` command will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.

### Loose
Allows you to specify a list of nodes that must be traversed when going to the destination.

### Strict
Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination.

### Record
Allows you to specify the number of hops to leave room for.

### Timestamp
Allows you to specify the number of time stamps to leave room for.

### Verbose
If you select any option, the verbose mode is automatically selected and the `trace` command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting.

The following table describes the characters that can appear in `trace` command output.

### Table 184: ip trace Text Characters

<table>
<thead>
<tr>
<th>Char</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nn</code> msec</td>
<td>For each node, the round-trip time (in milliseconds) for the specified number of probes.</td>
</tr>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>Char</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trace (user)</td>
<td>Discovers the CLNS routes that packets will actually take when traveling to their destination.</td>
</tr>
</tbody>
</table>

### trace (user)

To discover the IP routes that packets will actually take when traveling to their destination, use the `trace` command in EXEC mode.

```
trace [protocol] [destination]
```

#### Syntax Description

- **protocol** (Optional) Protocols that can be used are `appletalk`, `clns`, `ip` and `vines`.
- **destination** (Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

#### Command Default

The `protocol` argument is based on the Cisco IOS software examination of the format of the `destination` argument. For example, if the software finds a `destination` argument in IP format, the `protocol` defaults to `ip`.

#### Command Modes

EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The `trace` command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The `trace` command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The `trace` command sends several probes at each TTL level and displays the round-trip time for each.

The `trace` command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe
and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, `trace` prints an asterisk (*).

The `trace` command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type `Ctrl-^ X` by simultaneously pressing and releasing the `Ctrl`, `Shift`, and 6 keys, and then pressing the X key.

**Common Trace Problems**

Due to bugs in the IP implementation of various hosts and routers, the IP `trace` command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an ICMP message but they reuse the TTL of the incoming packet. Since this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the “ICMP” message can get back. For example, if the host is six hops away, `trace` will time out on responses 6 through 11.

**Trace IP Routes**

The following display shows sample IP `trace` output when a destination host name has been specified:

```
Router# trace ip ABA.NYC.mil
Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
  1 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
  2 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
  3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
  4 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
  5 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
  6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
  7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates the sequence number of the router in the path to the host.</td>
</tr>
<tr>
<td>DEBRIS.CISCO.COM</td>
<td>Host name of this router.</td>
</tr>
<tr>
<td>192.180.1.61</td>
<td>Internet address of this router.</td>
</tr>
<tr>
<td>1000 msec 8 msec 4 msec</td>
<td>Round-trip time for each of the three probes that are sent.</td>
</tr>
</tbody>
</table>

The following table describes the characters that can appear in `trace` output.

<table>
<thead>
<tr>
<th>Char</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nn msec</td>
<td>For each node, the round-trip time (in milliseconds) for the specified number of probes.</td>
</tr>
</tbody>
</table>
The probe timed out.

Unknown packet type.

Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.

Host unreachable.

Network unreachable.

Protocol unreachable.

Source quench.

Port unreachable.

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>trace (privileged)</strong></td>
<td>Probes the routes that packets follow when traveling to their destination from the router.</td>
</tr>
</tbody>
</table>

### traceroute

To discover the routes that packets will actually take when traveling to their destination address, use the **traceroute** command in user EXEC or privileged EXEC mode.

**traceroute**  
`[{{vrf vrf-name} topology topology-name}] [protocol] destination`

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies the name of a VPN virtual routing and forwarding (VRF) instance table in which to find the destination address. The only keyword that you can select for the <em>protocol</em> argument when you use the <code>vrf vrf-name</code> keyword-argument pair is the <em>ip</em> keyword.</td>
</tr>
<tr>
<td>topology topology-name</td>
<td>(Optional) Specifies the name of the topology instance. The <code>topology-name</code> argument is case-sensitive; “VOICE” and “voice” specify different topologies.</td>
</tr>
<tr>
<td>protocol</td>
<td>(Optional) Protocol keyword, either <code>appletalk</code>, <code>clns</code>, <code>ip</code>, <code>ipv6</code>, <code>ipx</code>, <code>oldvines</code>, or <code>vines</code>. When not specified, the <code>protocol</code> argument is based on an examination by the software of the format of the <code>destination</code> argument. The default protocol is IP.</td>
</tr>
<tr>
<td>destination</td>
<td>(Optional in privileged EXEC mode; required in user EXEC mode) The Destination address or hostname you want to trace of the route. The software determines the default parameters for the appropriate protocol and the tracing action begins.</td>
</tr>
</tbody>
</table>

### Command Default

When not specified, the `protocol` argument is determined by the software examining the format of the `destination` argument. For example, if the software finds a `destination` argument in IP format, the protocol value defaults to IP.

### Command Modes

User EXEC (>)
Privileged EXEC (#)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>The <code>vrf vrf-name</code> keyword and argument were added.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was modified, support for IPv6 was added.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was modified, support for IPv6 was added.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was modified, support for IPv6 was added.</td>
</tr>
<tr>
<td>12.2(11)T</td>
<td>The <code>traceroute</code> command test characters for IPv6 were updated. A new error message was added.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.3(5)</td>
<td>This command was modified, a line was added to the interactive <code>traceroute vrf</code> command, so that you can resolve the autonomous system number through the use of the global table or a VRF table, or you can choose not to resolve the autonomous system.</td>
</tr>
<tr>
<td>12.0(26)S1</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S1.</td>
</tr>
<tr>
<td>12.2(20)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(20)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>The <code>topology topology-name</code> keyword-argument pair was added to support Multitopology Routing (MTR).</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was modified. When the <code>vrf</code> keyword is used, the output displays the incoming VRF name/tag and the outgoing VRF name/tag.</td>
</tr>
<tr>
<td>15.0(1)SY</td>
<td>This command was modified. When the <code>vrf</code> keyword is used, the output displays the incoming VRF name/tag and the outgoing VRF name/tag.</td>
</tr>
<tr>
<td>15.2 (2)SNI</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `traceroute` command works by taking advantage of the error messages generated by devices when a datagram exceeds its hop limit value.

The `traceroute` command starts by sending probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring devices to discard the probe datagram and send back an error
message. The **traceroute** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A time-exceeded error message indicates that an intermediate device has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, simultaneously press and release the Ctrl, Shift, and 6 keys, and then pressing the X key.

To use non-default parameters and invoke an extended **traceroute** test, enter the command without a `protocol` or `destination` argument in privileged EXEC mode then follow a series of steps to select the desired parameters. Extended **traceroute** tests are not supported in user EXEC mode. The user-level **traceroute** feature provides a basic trace facility for users who do not have system privileges. The `destination` argument is required in user EXEC mode.

If the system cannot map an address for a hostname, it returns a “%No valid source address for destination” message.

If the `vrf vrf-name` keyword-argument pair is used, the `topology` option is not displayed because only the default VRF instance is supported. The `topology topology-name` keyword-argument pair and the DiffServ Code Point (DSCP) option in the extended **traceroute** system dialog are displayed only if a topology is configured on the device.

In Cisco IOS XE Release 3.2S, output of the **traceroute** command with the `vrf` keyword was enhanced to make troubleshooting easier by displaying the incoming VRF name/tag and the outgoing VRF name/tag.

### Examples

After you enter the **traceroute** command in privileged EXEC mode, the system prompts you for a protocol. The default protocol is IP.

If you enter a hostname or address on the same line as the **traceroute** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample output from the **traceroute** command using default values in privileged EXEC mode. The specific output varies somewhat from protocol to protocol.

```
Device# traceroute
Protocol [ip]:
Target IP address: Source address:
DSCP Value [0]: ! Only displayed if a topology is configured on the device.
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none]:
```

The following example displays output available in Cisco IOS XE Release 3.2S and later. Output of the **traceroute** command with the `vrf` keyword includes the incoming VRF name/tag and the outgoing VRF name/tag.

```
Device# traceroute vrf red 10.0.10.12
```
Type escape sequence to abort.
Tracing the route to 10.0.10.12
VRF info: (vrf in name/id, vrf out name/id)
1 10.1.13.15 (red/13,red/13) 0 msec
10.1.16.16 (red/13,red/13) 0 msec
10.1.13.15 (red/13,red/13) 1 msec
2 10.1.8.13 (red/13,red/13) 0 msec
10.1.7.13 (red/13,red/13) 0 msec
10.1.8.13 (red/13,red/13) 0 msec
3 10.1.2.11 (red/13,blue/10) 1 msec 0 msec 0 msec
4 * * *

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping (MTR)</td>
<td>Pings a destination within a specific topology for MTR.</td>
</tr>
</tbody>
</table>

**traceroute mac**

To display the Layer 2 path taken by the packets from the specified source to the specified destination, use the `traceroute mac` command in privileged EXEC mode.

```
traceroute mac source-mac-address {destination-mac-address|interface type interface-number destination-mac-address} [vlan vlan-id] [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-mac-address</td>
<td>Media Access Control (MAC) address of the source switch in hexadecimal format.</td>
</tr>
<tr>
<td>destination-mac-address</td>
<td>MAC address of the destination switch in hexadecimal format.</td>
</tr>
<tr>
<td>interface type</td>
<td>Specifies the interface where the MAC address resides; valid values are FastEthernet, GigabitEthernet, and Port-channel.</td>
</tr>
<tr>
<td>interface-number</td>
<td>Module and port number or the port-channel number; valid values for the port channel are from 1 to 282.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(Optional) Specifies the virtual local area network (VLAN) on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid values are from 1 to 4094.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed information about the Layer 2 trace.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the IP address where the MAC address resides.</td>
</tr>
<tr>
<td>source-ip-address</td>
<td>IP address of the source switch as a 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td>source-hostname</td>
<td>IP hostname of the source switch.</td>
</tr>
<tr>
<td>destination-ip-address</td>
<td>IP address of the destination switch as a 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td>destination-hostname</td>
<td>IP hostname of the destination switch.</td>
</tr>
</tbody>
</table>
This command has no default settings.

Privileged EXEC

Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA This command was integrated into Cisco IOS Release 12.2(33)SRA.

This command is not supported on the Cisco 7600 series router that is configured with a Supervisor Engine 2.

Do not use leading zeros when entering a VLAN ID.

For Layer 2 traceroute to functional properly, you must enable CDP on all of the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and a message appears.

The `traceroute mac` command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and a message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and a message appears.

When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute utility terminates at that hop and displays an error message.

This feature is not supported in Token Ring VLANs.

This example shows how to display detailed information about the Layer 2 path:

```
Router# traceroute mac 0001.0000.0204 0001.0000.0304 detail
Source 1001.0000.0204 found on VAYU[WS-C6509] (10.1.1.10)
  1 VAYU / WS-C6509 / 10.1.1.10 : Gi6/1 [full, 1000M] -> Po100 [auto, auto]
  2 PANI / WS-C6509 / 10.1.1.12 : Po100 [auto, auto] -> Po110 [auto, auto]
  3 BUMI / WS-C6509 / 10.1.1.13 : Po110 [auto, auto] -> Po120 [auto, auto]
  4 AGNI / WS-C6509 / 10.1.1.11 : Po120 [auto, auto] -> Gi8/12 [full, 1000M]
Destination 1001.0000.0304 found on AGNI[WS-C6509] (10.1.1.11)
Layer 2 trace completed.
Router#
```

This example shows the output when the switch is not connected to the source switch:

```
Router# traceroute mac 0001.0000.0204 0001.0000.0304
Destination 1001.0000.0304 not found
Router# traceroute mac 0001.0000.0204 0001.0000.0304
Layer 2 trace completed.
Router# traceroute mac 0001.0000.0204 0001.0000.0304
Layer 2 trace completed.
 Router#
Router# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ..... 
Source 1000.0201.0501 found on con5[WS-C6509] (10.2.5.5)
con5 / WS-C6509 / 10.2.5.5 :
  Fa0/1 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C6509 / 10.2.1.1 :
  G10/1 [auto, auto] =>G10/2 [auto, auto]
con2 / WS-C6509 / 10.2.2.2 :
  Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 1000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed.
Router#

This example shows the output when the switch cannot find the destination port for the source MAC address:

Router# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
Router#

This example shows the output when the source and destination devices are in different VLANs:

Router# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
Router#

This example shows the output when the destination MAC address is a multicast address:

Router# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Router#

This example shows the output when the source and destination switches belong to multiple VLANs:

Router# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
Router#

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

Router# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 1000.0201.0601 found on con6[WS-C6509] (10.2.6.6)
con6 (10.2.6.6) :Fa0/1 =>Fa0/3
con5 (10.2.5.5) :
  Fa0/3 =>Gi0/1
con1 (10.2.1.1) :
  Gi0/1 =>Gi0/2
con2 (10.2.2.2) :
  Gi0/2 =>Fa0/1
Destination 1000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed
Router#

This example shows how to display detailed traceroute information:

Router# traceroute mac ip 10.2.66.66 10.2.22.22 detail
Translating IP to mac.....
This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Router# traceroute mac ip con6 con2
Translating IP to mac ......
10.2.66.66 => 0000.0201.0601
10.2.22.22 => 0000.0201.0201
Source 0000.0201.0601 found on con6
con6 (10.2.6.6) : Fa0/1 => Fa0/3
con5 (10.2.5.5) : Fa0/3 => Gi0/1
con1 (10.2.1.1) : Gi0/1 => Gi0/2
con2 (10.2.2.2) : Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2 (10.2.2.2)
Layer 2 trace completed.
```

This example shows the output when ARP cannot associate the source IP address with the corresponding MAC address:

```
Router# traceroute mac ip 10.2.66.66 10.2.77.77
Arp failed for destination 10.2.77.77.
Layer2 trace aborted.
```

### undelete

To recover a file marked “deleted” on a Class A Flash file system, use the **undelete** command in user EXEC or privileged EXEC mode.

```
undelete index [filesystem :]
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>index</strong></td>
<td>A number that indexes the file in the <strong>dir</strong> command output.</td>
</tr>
<tr>
<td><strong>filesystem</strong></td>
<td>(Optional) A file system containing the file to undelete, followed by a colon.</td>
</tr>
</tbody>
</table>

**Command Default**

The default file system is the one specified by the **cd** command.

**Command Modes**

- user EXEC
- privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced for Class A Flash File Systems (platforms include the Cisco 7500 series and Cisco 12000 series).</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command was introduced on the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For Class A Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a “deleted” file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the “deleted” list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the `dir` command to learn the index number of the file you want to undelete.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked “deleted” on a Flash memory device, use the `squeeze` EXEC command.


Examples

In the following example, the deleted file at index 1 is recovered:

```
Router# show flash

System flash directory:
File  Length  Name/status
  1  8972116  c7000-js56i-mz.121-5.T [deleted]
  2  6765916  c7000-ds-mz.CSCds70452
[15738160 bytes used, 1039056 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
Router# undelete 1 flash:
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Deletes a file on a Flash memory device.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td>squeeze</td>
<td>Permanently deletes Flash files by squeezing a Class A Flash file system.</td>
</tr>
</tbody>
</table>
**unprofile**

To free the memory either by deleting data or disabling the profiles, use the `unprofile` command in privileged EXEC mode.

```
unprofile {process {process-ID process-name} {start-address end-address increment|all|task}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Sets the process specific information.</td>
</tr>
<tr>
<td>process-ID</td>
<td>Process ID. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td>process-name</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>start-address</td>
<td>Starting address of the profile.</td>
</tr>
<tr>
<td>end-address</td>
<td>Ending address of the profile.</td>
</tr>
<tr>
<td>increment</td>
<td>Incrementing address of the profile.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all profile data.</td>
</tr>
<tr>
<td>task</td>
<td>Disables task profiling.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SX1</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SX1.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to delete all the profile data:

```
Router# unprofile
    process all
```

**upgrade automatic abortversion**

To cancel the scheduled reloading of the device with a new Cisco software image, use the `upgrade automatic abortversion` command in privileged EXEC mode.

```
upgrade automatic abortversion
```
no upgrade automatic abortversion

Syntax Description
This command has no arguments or keywords.

Command Default
The reload of the device with the Cisco software image is not scheduled. The disk-management utility is disabled.

Command Modes
Privileged EXEC (#)

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use the upgrade automatic abortversion command to cancel a reload that has already been scheduled with either the upgrade automatic getversion command or the upgrade automatic runversion command.

Examples
The following example shows how to cancel a reload that is scheduled within one hour and 15 minutes. The reload was scheduled by using the upgrade automatic runversion command.

Device# upgrade automatic runversion in 01:15
Upgrading to "flash:c1841-adventerprisek9-mz.calvin-build-20060714". Wait..
Reload scheduled for 09:51:38 UTC Thu Aug 3 2006 (in 1 hour and 15 minutes) with image - flash:c1841-adventerprisek9-mz.calvin-build-20060714 by console
Reload reason: Auto upgrade
Device will WARM UPGRADE in 1:15:00
To cancel the upgrade, enter the command "upgrade automatic abortversion"
Device# upgrade automatic abortversion
Auto upgrade of image which was scheduled earlier is aborted!
***
*** --- SHUTDOWN ABORTED ---
***

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrade automatic getversion</td>
<td>Downloads a Cisco software image directly from <a href="http://www.cisco.com">www.cisco.com</a> or from a non-Cisco server.</td>
</tr>
<tr>
<td>upgrade automatic runversion</td>
<td>Reloads the device with a new Cisco software image.</td>
</tr>
</tbody>
</table>

upgrade automatic getversion
To download a Cisco software image directly from www.cisco.com or from a non-Cisco server, use the upgrade automatic getversion command in privileged EXEC mode.
upgrade automatic getversion {cisco username username password password image imageurl}
{{at hh:mm|now|in hh:mm}} [disk-management {auto|confirm|no}]

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Username for logging in to <a href="http://www.cisco.com">www.cisco.com</a>.</td>
</tr>
<tr>
<td>password</td>
<td>Password for logging in to <a href="http://www.cisco.com">www.cisco.com</a>.</td>
</tr>
<tr>
<td>image</td>
<td>Specifies the Cisco software image to which the device is to be upgraded.</td>
</tr>
<tr>
<td>url</td>
<td>URL from where the Cisco Auto-Upgrade Manager can download the image that</td>
</tr>
<tr>
<td></td>
<td>has already been downloaded to a non-Cisco server.</td>
</tr>
<tr>
<td>at</td>
<td>(Optional) Schedules a reload at a specified time. Use either of the following arguments with this keyword:</td>
</tr>
<tr>
<td></td>
<td>• hh:mm-- Hour and minute. The time entered must be in 24-hour format.</td>
</tr>
<tr>
<td></td>
<td>• now-- Immediately after the download of the Cisco software image.</td>
</tr>
<tr>
<td>in hh:mm</td>
<td>(Optional) Schedules a reload in a specified length of time after downloading the Cisco software image.</td>
</tr>
<tr>
<td>disk-management</td>
<td>(Optional) Cisco Auto-Upgrade Manager disk cleanup utility. You must configure one of the following keywords:</td>
</tr>
<tr>
<td></td>
<td>• auto --Deletes the files without asking for confirmation.</td>
</tr>
<tr>
<td></td>
<td>• confirm --Asks for confirmation before deleting a file.</td>
</tr>
<tr>
<td></td>
<td>• no --Never deletes any file.</td>
</tr>
</tbody>
</table>

Command Default

The reload of the device with the Cisco software image is not scheduled. The disk-management utility is disabled.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the upgrade automatic getversion command to download the Cisco software image to a device. You can either download the image from the Cisco website (www.cisco.com) or from a non-Cisco server to which the Cisco software image has already been downloaded from the Cisco website.

You can also use this command to schedule a reload. Additionally, this command can use the disk cleanup utility to delete files if there is not enough space to download the new Cisco software image.
**Downloading the Cisco Image from the Cisco Website**

The following example shows how to download a Cisco software image from the Cisco website (www.cisco.com). Here, the reloading of the device with the downloaded Cisco software image is not scheduled. Also, the disk-cleanup utility is not enabled.

Device# `upgrade automatic getversion cisco username myusername password mypassword image c3825-adventerprisek9-mz.124-2.XA.bin`

**Downloading the Cisco Image from a Non-Cisco TFTP Server**

The following example shows how to download the Cisco software image from a non-Cisco TFTP server and reload the device immediately after the download. It also shows how to delete the files automatically if there is not enough disk space.

Device# `upgrade automatic getversion tftp://abc/tom/c3825-adventerprisek9-mz.124-2.XA.bin at now disk-management auto`

**Downloading the Cisco Image from a Non-Cisco TFTP Server Using the Interactive Mode**

The following example shows how to use this command in interactive mode to download a Cisco software image from a non-Cisco server. Here, the reloading of the device with the downloaded Cisco software image is not scheduled.

Device# `upgrade automatic`

```
################################################################################
Welcome to the Cisco Auto Upgrade Manager. To upgrade your device, please answer the following questions. To accept the default value for a question, simply hit <ENTER>
################################################################################
Would you like to download an image directly from Cisco Server over the Internet? A valid Cisco login will be required.
Download from Cisco server? [yes]: no
Image location: tftp://10.1.0.1/emailid/c3825-adventerprisek9-mz_pi6_aum_review
Image Found: c3825-adventerprisek9-mz_pi6_aum_review (42245860 bytes)
Memory Available: 851Mb Main Memory (RAM) - 71335936 bytes of flash space
New image will be downloaded to flash:c3825-adventerprisek9-mz_pi6_aum_review [yes]: no
When would you like to reload your device? Use hh:mm format or specify "Manual" to not schedule a reload time. Use 'upgrade automatic runversion' to reload manually.
Time to reload the box [Manual]?
Proceed with device image upgrade from [tftp://10.1.0.1/emailid/c3825-adventerprisek9-mz_pi6_aum_review] to [c3825-adventerprisek9-mz_pi6_aum_review]? [yes]:
Downloading Image from user specified url: [tftp://10.1.0.1/emailid/c3825-adventerprisek9-mz_pi6_aum_review]
Loading emailid/c3825-adventerprisek9-mz_pi6_aum_review from 172.16.0.0(via GigabitEthernet0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 42245860 bytes]
[download complete]
Verifying the image: ......................
Done!
Image Verification: PASS
Use 'upgrade automatic runversion' command to reload manually.
```
upgrade automatic runversion

To reload the device with a new Cisco software image, use the `upgrade automatic runversion` command in privileged EXEC mode.

```
upgrade automatic runversion {at hh:mm | now in hh:mm}
```

### Syntax Description

<table>
<thead>
<tr>
<th>at</th>
<th>Schedules a reload at a specified time. Use either of the following arguments with this keyword:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>hh:mm</code>-- Hour and minute. The time entered must be in 24-hour format.</td>
</tr>
<tr>
<td></td>
<td>• <code>now</code>-- Immediately after the download of the Cisco software image.</td>
</tr>
</tbody>
</table>

| in | Schedules a reload in a specified length of time after downloading the Cisco software image. |

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `upgrade automatic runversion` command to schedule a reload after downloading a Cisco software image using the `upgrade automatic getversion` command.

You can also use the `upgrade automatic getversion` command to reload the device with the new Cisco software image. However, if you have already downloaded the Cisco software image using the `upgrade automatic getversion` command, you should use the `upgrade automatic runversion` command to reload the device.

### Examples

The following example shows how to schedule a reload after downloading a Cisco software image:

```
Device# show clock
09:01:36.124 UTC Thu Aug 3 2006
Device# upgrade automatic runversion at 10:20
Upgrading to "flash:c1841-adventerprisek9-mz.calvin-build-20060714". Wait..
Reload scheduled for 10:20:00 UTC Thu Aug 3 2006 (in 1 hour and 18 minutes) with image -
flash:c1841-adventerprisek9-mz.calvin-build-20060714 by console
Reload reason: Auto upgrade
Device will WARM UPGRADE at 10:20:00
```
To cancel the upgrade, enter the command "upgrade automatic abortversion"

Device#  

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrade automatic abortversion</td>
<td>Cancels upgrading the device with a new Cisco software image.</td>
</tr>
<tr>
<td>upgrade automatic getversion</td>
<td>Downloads a Cisco software image directly from <a href="http://www.cisco.com">www.cisco.com</a> or from a non-Cisco server.</td>
</tr>
</tbody>
</table>

**upgrade filesystem monlib**

To upgrade the ATA ROM monitor library (monlib) file without erasing file system data, use the `upgrade filesystem monlib` command in privileged EXEC mode.

```
upgrade filesystem monlib {disk0|disk1}
```

**Syntax Description**

- **disk0**: Selects disk 0 as the file system to be formatted.
- **disk1**: Selects disk 1 as the file system to be formatted.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC(#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2YST</td>
<td>This command was integrated into Cisco IOS Release 12.2YST.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you attempt to upgrade the ATA monlib file on a disk that has not been formatted on a router running Cisco IOS software, the upgrade operation will fail.

If the amount of space available on the disk for the monlib image is smaller than the monlib image you are trying to upgrade to, the upgrade operation will fail. The amount of space available for the monlib file can be determined by issuing the `show disk` command with the `all` keyword specified. The “Disk monlib size” field displays the number of bytes available for the ATA monlib file.

**Examples**

The following example shows how to upgrade the ATA monlib file on disk 0:

```
Router# upgrade filesystem monlib disk0
Hash Computation: 100%Done!
Computed Hash SHA2: DFBA872563104C8A7B7BF8158451F7F4
0AC333C98396D9DOE42DBD542C30E08
F3946DE692AF04F0B20F298E51C49C4
```
Digital signature successfully verified in file Monlib
Writing Monlib sectors....
Monlib write complete

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>format</td>
<td>Formats a Class A, Class B or Class C flash memory file system.</td>
</tr>
<tr>
<td>show disk</td>
<td>Displays flash or file system information for a disk.</td>
</tr>
</tbody>
</table>

**upgrade rom-monitor**

To set the execution preference on a read-only memory monitor (ROMMON), use the `upgrade rom-monitor` command in privileged EXEC or diagnostic mode.

```
upgrade rom-monitor slot num {sp|rp} file filename
upgrade rom-monitor slot num {sp|rp} {invalidate|preference} {region1|region2}
```

**Cisco ASR 1000 Series Aggregation Services Routers**

**upgrade rom-monitor filename URL slot**

**Syntax Description**

<table>
<thead>
<tr>
<th>slot num</th>
<th>Specifies the slot number of the ROMMON to be upgraded.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sp</td>
<td>Upgrades the ROMMON of the Switch Processor.</td>
</tr>
<tr>
<td>rp</td>
<td>Upgrades the ROMMON of the Route Processor.</td>
</tr>
<tr>
<td>file filename</td>
<td>Specifies the name of the S-record (SREC) file; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>invalidate</td>
<td>Invalidates the ROMMON of the selected region.</td>
</tr>
<tr>
<td>preference</td>
<td>Sets the execution preference on a ROMMON of the selected region.</td>
</tr>
<tr>
<td>region1</td>
<td>Selects the ROMMON in region 1.</td>
</tr>
<tr>
<td>region2</td>
<td>Selects the ROMMON in region 2.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the ROMMON package filename.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL to a ROMMON file. The URL always begins with a file system, such as bootflash:, harddisk:, obfl:, stby-harddisk:, or usbl[0-1], then specifies the path to the file.</td>
</tr>
</tbody>
</table>
The slot that contains the hardware that will receive the ROMMON upgrade. Options are:

- **number** -- the number of the Session Initiation Protocol (SIP) slot that requires the ROMMON upgrade
- **all** -- All hardware on the router
- **F0** -- Embedded-Service-Processor slot 0
- **F1** -- Embedded-Service-Processor slot 1
- **FP** -- All installed Embedded-Service-Processors
- **R0** -- Route-Processor slot 0
- **R1** -- Route-Processor slot 1
- **RP** -- Route-Processor

---

### Command Default

This command has no default settings.

### Command Modes

Privileged EXEC (#) Diagnostic (diag)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(24)T.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

**Caution**

If you enter the `upgrade rom-monitor` command from a Telnet session instead of a console connection, service may be interrupted.

The **slot num** keyword and argument combination is required for this command to function properly.

The **sp** or **rp** keyword is required if you installed a supervisor engine in the specified slot.

Valid values for **file filename** are the following:

- **bootflash:**
- **disk0:**
- **disk1:**
- **flash:**
On Cisco ASR 1000 Series Routers, this command can be used to upgrade ROMMON in privileged EXEC and diagnostic mode. The hardware receiving the ROMMON upgrade must be reloaded to complete the upgrade.

From Cisco IOS Release 12.4(24)T, you can use the `upgrade rom-monitor` command on Cisco 3200 series routers to upgrade ROMMON and the system bootstrap, if a newer version of ROMMON is available on the system.

**Examples**

This example shows how to upgrade the new ROMMON image to the flash device on a Supervisor Engine 2:

```
Router# upgrade rom-monitor
   slot 1 sp file tftp://dir1/tftpboot-users/A2_71059.srec
ROMMON image upgrade in progress
   Erasing flash
   Programming flash
   Verifying new image
   ROMMON image upgrade complete
   The card must be reset for this to take effect
```

In the following example, a ROMMON upgrade is performed to upgrade to Cisco IOS Release 12.2(33r)XN1 on a Cisco ASR 1000 Series Router using an ROMMON image stored on the bootflash: filesystem. All hardware is upgraded on the Cisco ASR 1000 Series Router in this example, and the router is then reloaded to complete the procedure.

```
Router# show rom-monitor 0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor F0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor R0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# copy tftp bootflash:
Address or name of remote host []? 127.23.16.81
Source filename []? auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg
Destination filename [asr1000-rommon.122-33r.XN1.pkg]? Accessing tftp://127.23.16.81/auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg...
Loading auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg from 127.23.16.81 (via GigabitEthernet0): !!!
[OK - 553164 bytes]
553164 bytes copied in 1.048 secs (527828 bytes/sec)
Router# dir bootflash:
```
Directory of bootflash:

11 drwx 16384 Dec 2 2004 12:02:09 +00:00 lost+found
14401 drwx 4096 Dec 2 2004 12:05:05 +00:00 .ssh
86401 drwx 4096 Dec 2 2004 12:05:07 +00:00 .rollback_timer
12 -rw- 33554432 Nov 20 2007 19:53:47 +00:00 nvram_00100
13 -rw- 6401536 Dec 23 2004 19:45:11 +00:00 mcp-fpd-pkg.122-test.pkg
28801 drwx 4096 Nov 1 2007 17:00:36 +00:00 .installer
15 -rw- 553164 Nov 28 2007 15:33:49 +00:00 asr1000-rommon.122-33r.XN1.pkg
16 -rw- 51716300 Nov 14 2007 16:39:59 +00:00 asr1000rp1-espbase.v122_33_xn_asr_rls0_throttle.pkg
17 -rw- 21850316 Nov 14 2007 16:41:23 +00:00 asr1000rp1-rpaccess-k9.v122_33_xn_asr_rls0_throttle.pkg
18 -rw- 21221580 Nov 14 2007 16:42:21 +00:00 asr1000rp1-rpcontrol.v122_33_xn_asr_rls0_throttle.pkg
19 -rw- 27576524 Nov 14 2007 16:43:50 +00:00 asr1000rp1-rpios-advipservicesk9.v122_33_xn_asr_rls0_throttle.pkg
20 -rw- 48478412 Nov 14 2007 16:45:50 +00:00 asr1000rp1-sipbase.v122_33_xn_asr_rls0_throttle.pkg
21 -rw- 36940208 Nov 14 2007 16:47:17 +00:00 asr1000rp1-sipspa.v122_33_xn_asr_rls0_throttle.pkg
22 -rw- 14749900 Nov 14 2007 16:48:17 +00:00 asr1000rp1-advipservicesk9.v122_33_xn_asr_rls0_throttle.pkg
23 -rw- 6049 Nov 14 2007 16:49:29 +00:00 packages.conf
24 -rw- 21325676 Nov 20 2007 19:53:13 +00:00 asr1000rp1-advipservicesk9.v122_33_xn_asr_rls0_throttle.bin
928833536 bytes total (451940352 bytes free)

Router# upgrade rom-monitor filename bootflash:/asr1000-rommon.122-33r.XN1.pkg all
Upgrade rom-monitor on Route-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Upgrade rom-monitor on Embedded-Service-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Upgrade rom-monitor on SPA-Inter-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608

ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Upgrade rom-monitor on SPA-Inter-Processor 1
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Router# reload
<reload bootup output removed for brevity>
Router# show rom-monitor 0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor F0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor R0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rom-monitor</td>
<td>Displays the ROMMON status.</td>
</tr>
</tbody>
</table>

upgrade filesystem monlib

To upgrade the ATA ROM monitor library (monlib) file without erasing file system data, use the upgrade filesystem monlib command in privileged EXEC mode.

upgrade filesystem monlib {disk0|disk1}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk0</td>
<td>Selects disk 0 as the file system to be formatted.</td>
</tr>
<tr>
<td>disk1</td>
<td>Selects disk 1 as the file system to be formatted.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values

Command Modes

Privileged EXEC(#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2YST</td>
<td>This command was integrated into Cisco IOS Release 12.2YST.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you attempt to upgrade the ATA monlib file on a disk that has not been formatted on a router running Cisco IOS software, the upgrade operation will fail.

If the amount of space available on the disk for the monlib image is smaller than the monlib image you are trying to upgrade to, the upgrade operation will fail. The amount of space available for the monlib file can be determined by issuing the `show disk` command with the `all` keyword specified. The “Disk monlib size” field displays the number of bytes available for the ATA monlib file.

Examples

The following example shows how to upgrade the ATA monlib file on disk 0:

```
Router# upgrade filesystem monlib disk0
Hash Computation: 100%Done!
Computed Hash SHA2: DFBA87256310DC8A7B7BF8158451F7F4
0AC333C9B396D90DE42DDB542C30E08
F3946DDE692AF04F0B20F29BE51C49C4
1B63179A542D81F9A7C90ABC2426960
Embedded Hash SHA2: DFBA87256310DC8A7B7BF8158451F7F4
0AC333C9B396D90DE42DDB542C30E08
F3946DDE692AF04F0B20F29BE51C49C4
1B63179A542D81F9A7C90ABC2426960
Digital signature successfully verified in file Monlib
Writing Monlib sectors....
Monlib write complete
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>format</td>
<td>Formats a Class A, Class B or Class C flash memory file system.</td>
</tr>
<tr>
<td>show disk</td>
<td>Displays flash or file system information for a disk.</td>
</tr>
</tbody>
</table>

upgrade rom-monitor preference

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR or Cisco 7301 router, use the `upgrade rom-monitor preference` command in privileged EXEC mode.

```
upgrade rom-monitor preference [{readonly|upgrade}]
```

Syntax Description

- **readonly** selects the ReadOnly ROMmon image to be booted on the next reload.
- **upgrade** selects the Upgrade second ROMmon image to be booted on the next reload.

Command Default

No default behavior or values

Command Modes

Privileged EXEC
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(28)S</td>
<td>This command was introduced on the Cisco 7200 VXR router.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router.</td>
</tr>
<tr>
<td>12.3(9)</td>
<td>This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

After running the upgrade rom-monitor preference command, you must reload the router for the selected ROMmon image to take effect.

Use the `rommon-pref` command when you are in ROMmon mode.

### Examples

The following example applicable to both the Cisco 7200 VXR and Cisco 7301 routers selects the ReadOnly ROMmon image to be booted on the next reload of the router:

```bash
Router# upgrade rom-monitor preference readonly
You are about to mark ReadOnly region of ROMMON for the highest boot preference.
Proceed? [confirm] Done! Router must be reloaded for this to take effect.
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rommon-pref</code></td>
<td>Selects a ReadOnly or Upgrade ROMmon image to be booted on the next reload when you are in ROMmon mode.</td>
</tr>
</tbody>
</table>

### vacant-message

To display an idle terminal message, use the `vacant-message` command in line configuration mode. To remove the default vacant message or any other vacant message that may have been set, use the `no` form of this command.

**vacant-message** 

`[d message d]`

**no vacant-message**

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>d</code></td>
<td>(Optional) Delimiting character that marks the beginning and end of the vacant-message. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote (&quot;), or tilde (~). ^C is reserved for special use and should not be used in the message.</td>
</tr>
<tr>
<td><code>message</code></td>
<td>(Optional) Vacant terminal message.</td>
</tr>
</tbody>
</table>

#### Command Default

The format of the default vacant message is as follows:

```
<blank lines>
hostname tty# is now available
<blank lines>
Press RETURN to get started.
```
This message is generated by the system.

Command Modes

Line configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command enables the banner to be displayed on the screen of an idle terminal. The `vacant-message` command without any arguments restores the default message.

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

For a rotary group, you need to define only the message for the first line in the group.

Examples

The following example turns on the system banner and displays this message:

```
Router(config)# line 0
Router(config-line)# vacant-message %
  Welcome to Cisco Systems, Inc.
  Press Return to get started.
```

verify

To verify the checksum of a file on a flash memory file system or compute a Message Digest 5 (MD5) signature for a file, use the `verify` command in privileged EXEC mode.

```
verify [/md5 [md5-value]] filesystem: [file-url]
```

Cisco 7600 Series Router

```
verify /[/md5 flash-filesystem [expected-md5-signature]]/ios flash-filesystem flash-filesystem
```

Syntax Description

<table>
<thead>
<tr>
<th>md5</th>
<th>(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5-value</td>
<td>(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system calculates the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.</td>
</tr>
<tr>
<td>filesystem :</td>
<td>File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are flash: and bootflash:.</td>
</tr>
</tbody>
</table>
### file-url
(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7600 Series Router</td>
<td>Computes an MD5 signature for a file; valid values are <code>bootflash:</code>, <code>disk0:</code>, <code>disk1:</code>, <code>flash:</code>, or <code>sup-bootflash:</code>.</td>
</tr>
<tr>
<td>/md5 flash-filesystem</td>
<td>(Optional) MD5 signature.</td>
</tr>
<tr>
<td>/ios flash-filesystem</td>
<td>Verifies the compressed Cisco IOS image checksum; valid values are <code>bootflash:</code>, <code>disk0:</code>, <code>disk1:</code>, <code>flash:</code>, or <code>sup-bootflash:</code>.</td>
</tr>
<tr>
<td>flash-filesystem</td>
<td>Device where the Flash memory resides; valid values are <code>bootflash:</code>, <code>disk0:</code>, <code>disk1:</code>, <code>flash:</code>, or <code>sup-bootflash:</code>.</td>
</tr>
</tbody>
</table>

### Command Default
The current working device is the default device (file system).

### Command Modes
Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>The <code>/md5</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>The <code>verify</code> command was enhanced to verify the hash that is contained in the image, and the output was enhanced to show the hash value in addition to the entire hash image (CCO hash).</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>The <code>verify</code> command enhancements were integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was added for the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The <code>verify</code> command enhancements were integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
This command replaces the `copy verify` and `copy verify flash` commands.

Use the `verify` command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into flash memory; it is not displayed when the image file is copied from one disk to another.

**Supported Platforms Other than the Cisco 7600 Series Router**

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into flash memory or onto a server. A variety of image information is available on Cisco.com. For example, you can get the Release, Feature Set, Size, BSD Checksum, etc.
Router Checksum, MD5, and Publication Date information by clicking on the image file name prior to downloading it from the Software Center on Cisco.com.

To display the contents of flash memory, use the `show flash` command. The flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into flash memory, use the `verify` command. Note, however, that the `verify` command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection. If a corrupt image is transferred successfully to the router, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the `verify` command with the `/md5` option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The `/md5` option of the `verify` command allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, issue the `verify` command using the `/md5` keyword. For example, issuing the `verify flash:c7200-is-mz.122-2.T.bin/md5` command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the `verify flash:c7200-is-mz.122-2.T.bin/md5 8b5f3062c4caec4a72571440e962233` command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

**Cisco 7600 Series Router**

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or onto a server.

Use the `verify /md5` command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature that is posted on the Cisco.com page with the image. You can use the `verify /md5` command in one of the following ways:

- Verify the MD5 signatures manually by entering the `verify /md5 filename` command.

Check the displayed signature against the MD5 signature that is posted on the Cisco.com page.

- Allow the system to compare the MD5 signatures by entering the `verify /md5 flash-filesystem:filename expected-md5-signature` command.

After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f
.
.
.
Done !
%Error verifying disk0:c6msfc2-jsv-mz
```
To display the contents of the flash memory, enter the `show flash` command. The listing of the flash contents does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the flash memory, enter the `verify` command.

A colon (:) is required after the specified device.

**Examples**

**Supported Platforms Other than Cisco 7600 Series Router**

The following example shows how to use the `verify` command to check the integrity of the file `c7200-js-mz` on the flash memory card inserted in slot 0:

```
Router# dir slot0:
Directory of slot0:/
    1 -rw- 4720148 Aug 29 1997 17:49:36 hampton/nitro/c7200-j-mz
    2 -rw- 4767328 Oct 01 1997 18:42:53 c7200-js-mz
    5 -rw-   639 Oct 02 1997 12:09:32 rally
    7 -rw-   639 Oct 02 1997 12:37:13 the_time
20578304 bytes total (3104544 bytes free)
Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

In the following example, the `/md5` keyword is used to display the MD5 value for the image:

```
Router# verify /md5 disk1:
Verify filename []? c7200-js-mz
.
.
.
Done
!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

In the following example, the known MD5 value for the image (obtained from Cisco.com) is specified in the `verify` command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz?
WORD Expected md5 signature
<cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.
.
Done
!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

```
The following example shows how the output of the `verify` command was enhanced to show the hash value in addition to the entire hash image (CCO hash):

Router# verify disk0:c7200-js-mz
%Filesystem does not support verify operations
```
Verifying file integrity of disk0:c7200-js-mz
.
.
.
Done
!
Embedded Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified

Cisco 7600 Series Router

This example shows how to check the MD5 signature manually:

Router# verify /md5 c6msfc2-jsv-mz
.
.
.
Done
!
verify /md5 (disk0:c6msfc2-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3

This example shows how to allow the system to compare the MD5 signatures:

Router# verify /md5 disk0:c6msfc2-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
.
.
.
Done
!
verified /md5 (disk0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#

This example shows how to verify the compressed checksum of the Cisco IOS image:

Router# verify /ios disk0:c6k222-jsv-mz
Verified compressed IOS image checksum for disk0:c6k222-jsv-mz

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the default directory or file system.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>copy /noverify</td>
<td>Disables the automatic image verification for the current copy operation.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>file verify auto</td>
<td>Verifies the compressed Cisco IOS image checksum.</td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current setting of the cd command.</td>
</tr>
<tr>
<td>show file systems</td>
<td>Lists available file systems.</td>
</tr>
<tr>
<td>show flash</td>
<td>Displays the layout and contents of flash memory.</td>
</tr>
</tbody>
</table>

### vtp

To configure the global VLAN Trunking Protocol (VTP) state, use the `vtp` command in global configuration mode. To return to the default value, use the `no` form of this command.

```plaintext
vtp [domain domain-name|file filename|interface interface-name [only]|mode {client|off|server|transparent} [vlan|mst|unknown]|password password-value [hidden|secret]]|pruning|version {1|2|3}]
```

#### Syntax Description

- **domain domain-name**: Sets the VTP administrative domain name.
- **file filename**: Sets the ASCII name of the IFS file system file where the VTP configuration is stored.
- **interface interface-name**: Sets the name of the preferred source for the VTP-updater ID for this device.
- **only**: (Optional) Specifies to use only this interface’s IP address as the VTP-IP updater address.
- **mode client**: Sets the type of VTP-device mode to client mode.
- **mode off**: Sets the type of VTP-device mode to off mode.
- **mode server**: Sets the type of VTP-device mode to server mode.
- **mode transparent**: Sets the type of VTP-device mode to transparent mode.
- **vlan**: Specifies VTP version 3 VLAN instances.
- **mst**: Specifies VTP version 3 MST instances.
- **unknown**: Specifies VTP version 3 for all other instances.
- **password password-value**: Specifies the administrative-domain password.
- **hidden**: (Optional) Specifies that the VTP version 3 secret key generated from the password be saved in the const_nvram:vlan.dat file.
- **secret**: (Optional) Allows you to directly configure the VTP version 3 password secret key.
- **pruning**: Enables the administrative domain to permit pruning.
version {1 | 2 | 3} Specifies the administrative-domain VTP version number.

The defaults are as follows:

- **vtp domain** and **vtp interface** commands have no default settings.
- **filename** is const-nvram:vlan.dat.
- VTP mode is **mode server** for VLANs and **transparent** for all other features.
- No password is configured.
- Pruning is disabled.
- Administrative-domain VTP version number 1.

Global configuration (config)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>The <strong>mode off</strong> keyword combination was added.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>Support for VTP version 3 was added.</td>
</tr>
</tbody>
</table>

The **vtp pruning**, **vtp password**, and **vtp version** commands are also available in privileged EXEC mode. We recommend that you use these commands in global configuration mode only; do not use these commands in privileged EXEC mode.

Extended-range VLANs are not supported by VTP.

When you define the domain-name value, the domain name is case sensitive and can be from 1 to 32 characters. The **filename** and **interface-name** values are ASCII strings from 1 to 255 characters.

You must configure a password on each network device in the management domain when the switch is in secure mode.

If you configure VTP in secure mode, the management domain does not function properly if you do not assign a management domain password to each network device in the domain.
A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).

Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.

In a Token Ring environment, you must enable VTP version 2 for VLAN switching to function properly.

Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.

Configuring VLANs as pruning eligible or pruning ineligible on a Cisco 7600 series router affects pruning eligibility for those VLANs on that switch only; it does not affect pruning eligibility on all network devices in the VTP domain.

The `vtp password`, `vtp pruning`, and `vtp version` commands are not placed in startup memory but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

You can configure the `pruning` keyword in VTP-server mode; the `version` keyword is configurable in VTP-server mode or VTP transparent mode.

The password-value argument is an ASCII string from 8 to 64 characters identifying the administrative domain for the device.

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

All Cisco 7600 series routers in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on Cisco 7600 series routers in the same VTP domain.

If all Cisco 7600 series routers in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one Cisco 7600 series router; the version number is then propagated to the other version 2-capable Cisco 7600 series routers in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified.

If you enter the `vtp mode off` command, it sets the device to off. If you enter the `no vtp mode off` command, it resets the device to the VTP server mode.

In VTP version 3, the VTP mode has to be specified on a per-feature basis. Use the `vlan` and `mst` keywords to configure the VTP mode on VLAN and MST instances. To configure the VTP mode for any other feature, use the `unknown` keyword. When you convert from either VTP version 1 or 2 to version 3, the current mode configuration will be preserved.

With VTP version 3, a new method is available for hiding the VTP password from the configuration file. When you use the `hidden` keyword, the secret key that is generated from the password string is saved in the `const_nvravm:vlan.dat` file. If you use the `secret` keyword, you can directly configure the password secret key. By using the `secret` keyword, you can distribute the password in the secret key format rather than in the cleartext format.

**Examples**

This example shows how to set the device’s management domain:

```
Router(config)#
vtp domain DomainName1
```
This example shows how to specify the file in the IFS-file system where the VTP configuration is stored:

```
Router(config)#
vtp file vtpconfig
```

Setting device to store VLAN database at filename vtpconfig.

This example shows how to set the VTP mode to client:

```
Router(config)#
vtp mode client
```

Setting device to VTP CLIENT mode.

This example shows how to disable VTP mode globally:

```
Router(config)# vtp mode off
```

Setting device to VTP OFF mode.

This example shows how to reset the device to the VTP server mode:

```
Router(config)# no vtp mode off
```

Setting device to VTP OFF mode.

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vtp</td>
<td>Displays the VTP statistics and domain information.</td>
</tr>
<tr>
<td>vtp (interface configuration)</td>
<td>Enables VTP on a per-port basis.</td>
</tr>
</tbody>
</table>

---

### warm-reboot

To enable a router to do a warm-reboot, use the `warm-reboot` command in global configuration mode. To disable warm rebooting, use the `no` form of this command.

```
warm-reboot [count number] [uptime minutes]
no warm-reboot count number uptime minutes
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>count number</strong></td>
</tr>
<tr>
<td>(Optional) Maximum number of warm reboots allowed between any intervening cold reboot. Valid values range from 1 to 50. The default value is 5 times.</td>
</tr>
<tr>
<td><strong>uptime minutes</strong></td>
</tr>
<tr>
<td>(Optional) Minimum number of minutes that must elapse between initial system configuration and an exception before a warm reboot is attempted. If the system crashes before the specified time elapses, a warm reboot is not attempted. Valid values range from 0 to 120. The default value is 5 minutes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warm rebooting is disabled.</td>
</tr>
</tbody>
</table>

If warm rebooting is enabled, the default value for the **count number** option is 5 times, and the default value for the **uptime minutes** option is 5 minutes.

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration</td>
</tr>
</tbody>
</table>
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `warm-reboot` command to enable the router to reload a Cisco IOS image without ROM monitor mode (ROMMON) intervention, in which the image restores read-write data from a previously saved copy in the RAM and starts execution from that point. Unlike a cold reboot, this process does not involve a flash to RAM copy or self-decompression of the image.

**Note**

After a warm reboot is enabled, it will not become active until after the next cold reboot because a warm reboot requires a copy of the initialized memory.

**Note**

If the system crashes before the image completes the warm reboot process, a cold reboot is initiated.

**Examples**

The following example shows how to enable a warm reboot on the router:

```
Router#(config) warm-reboot count 10 uptime 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show warm-reboot</code></td>
<td>Displays the statistics for attempted warm reboots.</td>
</tr>
</tbody>
</table>

**where**

To list the open sessions, use the `where` command in EXEC mode.

```
where
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced in a release prior to Cisco IOS Release 10.0.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `where` command displays all open sessions associated with the current terminal line.
The break (Ctrl-Shift-6, x), where, and resume commands are available with all supported connection protocols.

**Examples**

The following is sample output from the `where` command:

```
Router# where
Conn Host Address Byte Idle Conn Name
  1 MATHOM 192.31.7.21 0 0 MATHOM
* 2 CHAFF 131.108.12.19 0 0 CHAFF
```

The asterisk (*) indicates the current terminal session.

The following table describes the fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conn</td>
<td>Name or address of the remote host to which the connection is made.</td>
</tr>
<tr>
<td>Host</td>
<td>Remote host to which the router is connected through a Telnet session.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the remote host.</td>
</tr>
<tr>
<td>Byte</td>
<td>Number of unread bytes for the user to see on the connection.</td>
</tr>
<tr>
<td>Idle</td>
<td>Interval (in minutes) since data was last sent on the line.</td>
</tr>
<tr>
<td>Conn Name</td>
<td>Assigned name of the connection.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show line</td>
<td>Displays information about all lines on the system or the specified line.</td>
</tr>
<tr>
<td>show sessions</td>
<td>Displays information about open LAT, Telnet, or rlogin connections.</td>
</tr>
</tbody>
</table>

**width**

To set the terminal screen width, use the `width` command in line configuration mode. To return to the default screen width, use the `no` form of this command.

```
width characters
no width
```

**Syntax Description**

| characters | Number of character columns displayed on the terminal. The default is 80 characters. |

**Command Default**

80 character columns

**Command Modes**

Line configuration
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Usage Guidelines

By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal.

The rlogin protocol uses the value of the characters argument to set up terminal parameters on a remote host.

Examples

In the following example the location for line 7 is defined as “console terminal” and the display is set to 132 columns wide:

```
Router(config)# line 7
Router(config-line)# location console terminal
Router(config-line)# width 132
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal width</td>
<td>Sets the number of character columns on the terminal screen for the current session.</td>
</tr>
</tbody>
</table>

write core

To test the configuration of a core dump setup, use the `write core` command in privileged EXEC mode.

```
write core [{hostname [LINE]}destination-address [LINE]]
```

Syntax Description

- `hostname` (Optional) Host name of the remote server where the core dump file is to be written.
- `destination-address` (Optional) IP address of the remote server where the core dump file is to be written.
- `LINE` (Optional) Assigns the name “LINE” to the core dump file.

Command Default

If the `hostname` or `destination-address` arguments are not specified, the core dump file is written to the IP address or hostname specified by the `exception dump` command.

If the `LINE` keyword is not specified, the name of the core dump file is assigned as the host name of the remote server followed by the word “-core.”

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When a router reloads, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the reload. Core dumps are generally useful to your technical support representative. Not all types of router reloads will produce a core dump.
The **write core** command causes the router to generate a core dump without reloading, which may be useful if the router is malfunctioning but has not reloaded. The core dump files will be the size of the respective memory regions. It is important to remember that the entire memory region is dumped, not just the memory that is in use.

⚠️ **Caution**

Use the **write core** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. When using this command, the router will not reload until the content of its memory is dumped. This event might take some time, depending on the amount of DRAM present on the router. Also, the resulting binary file, which is very large, must be transferred to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel who have access to source code and detailed memory maps.

Depending on your TFTP server, you might need to create an empty target file to which the router can write the core dump.

**Examples**

The following example shows how to test the configuration of a core dump setup. In this example, the core dump file is written to the remote server with the host name test.

```plaintext
write core test
```

**write erase**

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command for more information.

**write memory**

To save the running configuration to the nonvolatile random-access memory (NVRAM), use the **write memory** command in privileged EXEC mode.

```plaintext
write memory
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)T</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.2(11)T.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(14)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

If you try to configure the `write memory` command when a router is low on memory and the backup buffer cannot be allocated, then the command will fail with the error message, “Not enough space.” When the `write memory` command fails to apply the new configuration, the backup configuration is used to restore the original configuration.

**Examples**

The following example shows how to save the running configuration to NVRAM:

```
Router> enable
Router# write memory
```

**write mib-data**

To save MIB data to system memory (NVRAM) for MIB Data Persistence, use the `write mib-data` command in EXEC mode.

```
write mib-data
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The MIB Data Persistence feature allows the SNMP data of a MIB to be persistent across reloads; that is, the values of certain MIB objects are retained even if your networking device reboots.

To determine which MIBs support “MIB Persistence” in your release, use the `snmp mib persist` command in global configuration mode.

Any modified MIB data must be written to NVRam memory using the `write mib-data` command. If the `write mib-data` command is not used, modified MIB data is not saved automatically, even if MIB Persistence is enabled. Executing the `write mib-data` command saves only the current MIB data; if the MIB object values are changed, you should reenter the `write mib-data` command to ensure that those values are persistent across reboots.

**Examples**

The following example shows the enabling of event MIB persistence, circuit MIB persistence, and saving the changes to set object values for these MIBs to NVRAM:
Router# configure terminal
Router(config)# snmp mib persist circuit
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp mib persist</td>
<td>Enables MIB data persistence.</td>
</tr>
</tbody>
</table>

**write network**

This command has been replaced by `copy system:/running-config` command.

To upload the current configuration to the network, use the `write network` command in privileged EXEC mode.

```
write network [host-file-address]
```

**Syntax Description**

| host-file-address | (Optional) Address of the host file to be uploaded. |

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `write network` command cannot be used to upload software to the ATM module.

**Examples**

This example shows how to upload the system5.cfg file to the mercury host using the `write network` command:

```
Router# write network
IP address or name of host? mercury
Name of configuration file to write? system5.cfg
```
Upload configuration to system5.cfg on mercury (y/n) [y]? y
Done. Finished Network Upload. (9003 bytes)

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy</td>
<td>Copies files from a source to specified destination.</td>
</tr>
<tr>
<td></td>
<td>show config</td>
<td>Displays the nondefault or module configuration information.</td>
</tr>
</tbody>
</table>

### write terminal

This command is deprecated. Deprecated commands are considered obsolete, and their use is discouraged. Support for this command may be removed.

The `write terminal` command is now enabled only as a command alias for the `show running-config` command.

The `show running-config` command offers additional options not available for the `write terminal` command; see the documentation of the `show running-config` command for details.

#### Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0</td>
<td>This command was introduced in a release prior to 8.0.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>show running-config</code> command was introduced as a replacement for the <code>write terminal</code> command.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### xmodem

To copy a Cisco IOS image to a router using the ROM monitor and the Xmodem or Ymodem protocol, use the `xmodem` command in ROM monitor mode.

```
.xmodem [-c] [-y] [-e] [-f] [-r] [-x] [-s] [data-rate] [filename]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>(Optional) CRC-16 checksumming, which is more sophisticated and thorough than standard checksumming.</td>
</tr>
<tr>
<td>-y</td>
<td>(Optional) Uses the Ymodem protocol for higher throughput.</td>
</tr>
<tr>
<td>-e</td>
<td>(Optional) Erases the first partition in Flash memory before starting the download. This option is only valid for the Cisco 1600 series.</td>
</tr>
<tr>
<td>-f</td>
<td>(Optional) Erases all of Flash memory before starting the download. This option is only valid for the Cisco 1600 series.</td>
</tr>
<tr>
<td>-r</td>
<td>(Optional) Downloads the file to DRAM. The default is Flash memory.</td>
</tr>
</tbody>
</table>
-x  (Optional) Do not execute Cisco IOS image on completion of the download.

-s  data-rate  (Optional) Sets the console port’s data rate during file transfer. Values are 1200, 2400, 4800, 9600, 19200, 38400, and 115200 bps. The default rate is specified in the configuration register. This option is only valid for the Cisco 1600 series.

filename  (Optional) Filename to copy. This argument is ignored when the -r keyword is specified, because only one file can be copied to DRAM. On the Cisco 1600 series routers, files are loaded to the ROM for execution.

**Command Default**

Xmodem protocol with 8-bit CRC, file downloaded into Flash memory and executed on completion.

**Command Modes**

ROM monitor

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Cisco 3600 series routers does not support XBOOT functionality. If your Cisco IOS image is erased or damaged, you cannot load a new image over the network.

Use the `xmodem` ROM monitor command to download a new system image to your router from a local personal computer (such as a PC, Mac, or UNIX workstation), or a remote computer over a modem connection, to the router’s console port. The computer must have a terminal emulation application that supports these protocols.

**Cisco 3600 Series Routers**

Your router must have enough DRAM to hold the file being transferred, even if you are copying to Flash memory. The image is copied to the first file in internal Flash memory. Any existing files in Flash memory are erased. There is no support for partitions or copying as a second file.

**Cisco 1600 Series Routers**

If you include the -r option, your router must have enough DRAM to hold the file being transferred. To run from Flash, an image must be positioned as the first file in Flash memory. If you are copying a new image to boot from Flash, erase all existing files first.

**Caution**

A modem connection from the telephone network to your console port introduces security issues that you should consider before enabling the connection. For example, remote users can dial in to your modem and access the router’s configuration settings.

**Note**

If the file to be downloaded is not a valid router image, the copy operation is automatically terminated.

**Examples**

The following example uses the `xmodem -c filename` ROM monitor command to copy the file named `new-ios-image` from a remote or local computer:
common > xmodem -c new-ios-image
Do not start the sending program yet...

    File size  Checksum   File name
          1738244 bytes (0x1a8604)  0xdd25 george-admin/c3600-i-mz
WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: yes
Ready to receive file new-ios-image ...

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>copy xmodem:</strong></td>
<td>Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol.</td>
</tr>
<tr>
<td><strong>copy ymodem:</strong></td>
<td>Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol.</td>
</tr>
</tbody>
</table>
ASCII Character Set and Hexadecimal Values

• ASCII Character Set and Hexadecimal Values, on page 1114
ASCII Character Set and Hexadecimal Values

Some commands described in the Cisco IOS documentation set, such as the escape-character line configuration command, require that you enter the decimal representation of an ASCII character. Other commands occasionally make use of hexadecimal (hex) representations.

The below table provides character code translations from the decimal numbers to their hexadecimal and ASCII equivalents. It also provides the keyword entry for each ASCII character. For example, the ASCII carriage return (CR) is decimal 13. Entering Ctrl-M at your terminal generates decimal 13, which is interpreted as a CR.

---

**Note**

This document is a reference for only the standard ASCII character set. Extended ASCII character sets are not generally recommended for use in Cisco IOS commands. Extended ASCII character set references are widely available on the internet.

---

**Table 188: ASCII Translation Table**

<table>
<thead>
<tr>
<th>Numeric Values</th>
<th>ASCII Character</th>
<th>Meaning</th>
<th>Keyboard Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>Hex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>NUL</td>
<td>Null</td>
</tr>
<tr>
<td>1</td>
<td>01</td>
<td>SOH</td>
<td>Start of heading</td>
</tr>
<tr>
<td>2</td>
<td>02</td>
<td>STX</td>
<td>Start of text</td>
</tr>
<tr>
<td>3</td>
<td>03</td>
<td>ETX</td>
<td>Break/end of text</td>
</tr>
<tr>
<td>4</td>
<td>04</td>
<td>EOT</td>
<td>End of transmission</td>
</tr>
<tr>
<td>5</td>
<td>05</td>
<td>ENQ</td>
<td>Enquiry</td>
</tr>
<tr>
<td>6</td>
<td>06</td>
<td>ACK</td>
<td>Positive acknowledgment</td>
</tr>
<tr>
<td>7</td>
<td>07</td>
<td>BEL</td>
<td>Bell</td>
</tr>
<tr>
<td>8</td>
<td>08</td>
<td>BS</td>
<td>Backspace</td>
</tr>
<tr>
<td>9</td>
<td>09</td>
<td>HT</td>
<td>Horizontal tab</td>
</tr>
<tr>
<td>10</td>
<td>0A</td>
<td>LF</td>
<td>Line feed</td>
</tr>
<tr>
<td>11</td>
<td>0B</td>
<td>VT</td>
<td>Vertical tab</td>
</tr>
<tr>
<td>12</td>
<td>0C</td>
<td>FF</td>
<td>Form feed</td>
</tr>
<tr>
<td>13</td>
<td>0D</td>
<td>CR</td>
<td>Carriage return (in the CLI, equivalent to the Enter or Return key)</td>
</tr>
<tr>
<td>14</td>
<td>0E</td>
<td>SO</td>
<td>Shift out</td>
</tr>
</tbody>
</table>

---

Cisco IOS Configuration Fundamentals Command Reference
<table>
<thead>
<tr>
<th>Numeric Values</th>
<th>ASCII Character</th>
<th>Meaning</th>
<th>Keyboard Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0F</td>
<td>SI</td>
<td>Shift in/XON (resume output)</td>
</tr>
<tr>
<td>16</td>
<td>10</td>
<td>DLE</td>
<td>Data link escape</td>
</tr>
<tr>
<td>17</td>
<td>11</td>
<td>DC1</td>
<td>Device control character 1</td>
</tr>
<tr>
<td>18</td>
<td>12</td>
<td>DC2</td>
<td>Device control character 2</td>
</tr>
<tr>
<td>19</td>
<td>13</td>
<td>DC3</td>
<td>Device control character 3</td>
</tr>
<tr>
<td>20</td>
<td>14</td>
<td>DC4</td>
<td>Device control character 4</td>
</tr>
<tr>
<td>21</td>
<td>15</td>
<td>NAK</td>
<td>Negative acknowledgment</td>
</tr>
<tr>
<td>22</td>
<td>16</td>
<td>SYN</td>
<td>Synchronous idle</td>
</tr>
<tr>
<td>23</td>
<td>17</td>
<td>ETB</td>
<td>End of transmission block</td>
</tr>
<tr>
<td>24</td>
<td>18</td>
<td>CAN</td>
<td>Cancel</td>
</tr>
<tr>
<td>25</td>
<td>19</td>
<td>EM</td>
<td>End of medium</td>
</tr>
<tr>
<td>26</td>
<td>1A</td>
<td>SUB</td>
<td>Substitute/end of file</td>
</tr>
<tr>
<td>27</td>
<td>1B</td>
<td>ESC</td>
<td>Escape</td>
</tr>
<tr>
<td>28</td>
<td>1C</td>
<td>FS</td>
<td>File separator</td>
</tr>
<tr>
<td>29</td>
<td>1D</td>
<td>GS</td>
<td>Group separator</td>
</tr>
<tr>
<td>30</td>
<td>1E</td>
<td>RS</td>
<td>Record separator</td>
</tr>
<tr>
<td>31</td>
<td>1F</td>
<td>US</td>
<td>Unit separator</td>
</tr>
<tr>
<td>32</td>
<td>20</td>
<td>SP</td>
<td>Space</td>
</tr>
<tr>
<td>33</td>
<td>21</td>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>34</td>
<td>22</td>
<td>&quot;</td>
<td>&quot;</td>
</tr>
<tr>
<td>35</td>
<td>23</td>
<td>#</td>
<td>#</td>
</tr>
<tr>
<td>36</td>
<td>24</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>37</td>
<td>25</td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>38</td>
<td>26</td>
<td>&amp;</td>
<td>&amp;</td>
</tr>
<tr>
<td>39</td>
<td>27</td>
<td>'</td>
<td>'</td>
</tr>
<tr>
<td>40</td>
<td>28</td>
<td>(</td>
<td>(</td>
</tr>
<tr>
<td>41</td>
<td>29</td>
<td>)</td>
<td>)</td>
</tr>
<tr>
<td>42</td>
<td>2A</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Numeric Values</td>
<td>ASCII Character</td>
<td>Meaning</td>
<td>Keyboard Entry</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>43</td>
<td>2B</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>44</td>
<td>2C</td>
<td>,</td>
<td>,</td>
</tr>
<tr>
<td>45</td>
<td>2D</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>46</td>
<td>2E</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>47</td>
<td>2F</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>48</td>
<td>30</td>
<td>0 Zero</td>
<td>0</td>
</tr>
<tr>
<td>49</td>
<td>31</td>
<td>1 One</td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>32</td>
<td>2 Two</td>
<td>2</td>
</tr>
<tr>
<td>51</td>
<td>33</td>
<td>3 Three</td>
<td>3</td>
</tr>
<tr>
<td>52</td>
<td>34</td>
<td>4 Four</td>
<td>4</td>
</tr>
<tr>
<td>53</td>
<td>35</td>
<td>5 Five</td>
<td>5</td>
</tr>
<tr>
<td>54</td>
<td>36</td>
<td>6 Six</td>
<td>6</td>
</tr>
<tr>
<td>55</td>
<td>37</td>
<td>7 Seven</td>
<td>7</td>
</tr>
<tr>
<td>56</td>
<td>38</td>
<td>8 Eight</td>
<td>8</td>
</tr>
<tr>
<td>57</td>
<td>39</td>
<td>9 Nine</td>
<td>9</td>
</tr>
<tr>
<td>58</td>
<td>3A</td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>59</td>
<td>3B</td>
<td>;</td>
<td>;</td>
</tr>
<tr>
<td>60</td>
<td>3C</td>
<td>&lt;</td>
<td>&lt;</td>
</tr>
<tr>
<td>61</td>
<td>3D</td>
<td>=</td>
<td>=</td>
</tr>
<tr>
<td>62</td>
<td>3E</td>
<td>&gt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>63</td>
<td>3F</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>64</td>
<td>40</td>
<td>@</td>
<td>@</td>
</tr>
<tr>
<td>65</td>
<td>41</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>66</td>
<td>42</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>67</td>
<td>43</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>68</td>
<td>44</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>69</td>
<td>45</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>70</td>
<td>46</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Numeric Values</td>
<td>ASCII Character</td>
<td>Meaning</td>
<td>Keyboard Entry</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>71</td>
<td>47</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>72</td>
<td>48</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>73</td>
<td>49</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>74</td>
<td>4A</td>
<td>J</td>
<td>J</td>
</tr>
<tr>
<td>75</td>
<td>4B</td>
<td>K</td>
<td>K</td>
</tr>
<tr>
<td>76</td>
<td>4C</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>77</td>
<td>4D</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>78</td>
<td>4E</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>79</td>
<td>4F</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>80</td>
<td>50</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>81</td>
<td>51</td>
<td>Q</td>
<td>Q</td>
</tr>
<tr>
<td>82</td>
<td>52</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>83</td>
<td>53</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>84</td>
<td>54</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>85</td>
<td>55</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>86</td>
<td>56</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>87</td>
<td>57</td>
<td>W</td>
<td>W</td>
</tr>
<tr>
<td>88</td>
<td>58</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>89</td>
<td>59</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>90</td>
<td>5A</td>
<td>Z</td>
<td>Z</td>
</tr>
<tr>
<td>91</td>
<td>5B</td>
<td>[</td>
<td>[</td>
</tr>
<tr>
<td>92</td>
<td>5C</td>
<td>\</td>
<td>\</td>
</tr>
<tr>
<td>93</td>
<td>5D</td>
<td>]</td>
<td>]</td>
</tr>
<tr>
<td>94</td>
<td>5E</td>
<td>^</td>
<td>^</td>
</tr>
<tr>
<td>95</td>
<td>5F</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>96</td>
<td>60</td>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td>97</td>
<td>61</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>98</td>
<td>62</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>Numeric Values</td>
<td>ASCII Character</td>
<td>Meaning</td>
<td>Keyboard Entry</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>99</td>
<td>63</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>100</td>
<td>64</td>
<td>d</td>
<td>d</td>
</tr>
<tr>
<td>101</td>
<td>65</td>
<td>e</td>
<td>e</td>
</tr>
<tr>
<td>102</td>
<td>66</td>
<td>f</td>
<td>f</td>
</tr>
<tr>
<td>103</td>
<td>67</td>
<td>g</td>
<td>g</td>
</tr>
<tr>
<td>104</td>
<td>68</td>
<td>h</td>
<td>h</td>
</tr>
<tr>
<td>105</td>
<td>69</td>
<td>i</td>
<td>i</td>
</tr>
<tr>
<td>106</td>
<td>6A</td>
<td>j</td>
<td>j</td>
</tr>
<tr>
<td>107</td>
<td>6B</td>
<td>k</td>
<td>k</td>
</tr>
<tr>
<td>108</td>
<td>6C</td>
<td>l</td>
<td>l</td>
</tr>
<tr>
<td>109</td>
<td>6D</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>110</td>
<td>6E</td>
<td>n</td>
<td>n</td>
</tr>
<tr>
<td>111</td>
<td>6F</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>112</td>
<td>70</td>
<td>p</td>
<td>p</td>
</tr>
<tr>
<td>113</td>
<td>71</td>
<td>q</td>
<td>q</td>
</tr>
<tr>
<td>114</td>
<td>72</td>
<td>r</td>
<td>r</td>
</tr>
<tr>
<td>115</td>
<td>73</td>
<td>s</td>
<td>s</td>
</tr>
<tr>
<td>116</td>
<td>74</td>
<td>t</td>
<td>t</td>
</tr>
<tr>
<td>117</td>
<td>75</td>
<td>u</td>
<td>u</td>
</tr>
<tr>
<td>118</td>
<td>76</td>
<td>v</td>
<td>v</td>
</tr>
<tr>
<td>119</td>
<td>77</td>
<td>w</td>
<td>w</td>
</tr>
<tr>
<td>120</td>
<td>78</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>121</td>
<td>79</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>122</td>
<td>7A</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>123</td>
<td>7B</td>
<td>{</td>
<td>{</td>
</tr>
<tr>
<td>124</td>
<td>7C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>7D</td>
<td>}</td>
<td>}</td>
</tr>
<tr>
<td>126</td>
<td>7E</td>
<td>~</td>
<td>~</td>
</tr>
<tr>
<td>Numeric Values</td>
<td>ASCII Character</td>
<td>Meaning</td>
<td>Keyboard Entry</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>127</td>
<td>7F</td>
<td>DEL</td>
<td>Delete</td>
</tr>
</tbody>
</table>