Cisco Security MARS Command Reference

Release 6.x
October 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16551-02

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Security MARS Command Reference

CONTENTS

Preface

Revised: October 15, 2010, OL-16551-02

Organization

This guide includes the following sections:

Section	Title	Description
1	Cisco Security MARS Command Reference —Commands A through V	Describes Cisco Security MARS command line interface commands, A–Z

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Command Privileges and Modes

To access the CLI on the MARS Appliance, you must have a console connection to the appliance and use the system administrative account, pnadmin. No other administrative account defined in the web interface has privileges to access the console connection. For more information about establishing a console connection, see Establishing a Console Connection.

Note There is only one command mode for the MARS Appliances.

CLI Conventions

The CLI uses the following conventions:

- The key combination **^C**, or **Ctrl-C**, means hold down the **Ctrl** key while you press the **C** key.
- A string is defined as a nonquoted set of characters.

Checking Command Syntax

The serial console interface provides several types of responses to incorrect command entries:

Command Line Entry	System Display
Command line that does not contain any valid commands.	`Unknown command`
Valid command that does not contain required options.	`Incomplete command`
Valid command that does not provide valid options or parameters.	`Invalid input`

In addition, some commands have command-specific error messages that notify you when a command is valid, but cannot run correctly.

System Help

You can obtain help using the following methods:

- For a list of all commands and a brief description, enter **help** or **?**, and then press **Enter**.
- For syntax help on a specific command, type the command name, a space, a dash, and a lowercase **h**, and then press **Enter**, for example, **arp -h**. The help contains command usage information and syntax.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Related Documentation

See, *Cisco Security MARS 6.x Documentation Guide and Warranty* at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/roadmap/map60x.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Cisco Security MARS Command Reference —Commands A through V

Revised: October 15, 2010, OL-16551-02

Command Summary

Table 1-1 summarizes all commands available on the MARS Appliance. Refer to the full description of commands that you are not familiar with before using them.

Note For MARS Releases prior to 6.0.1, the command reference is a chapter of the Install and Setup guide. This command reference documents only commands found in MARS Release 6.x.

Table 1-1 Command Summary

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
?	—	Print list of available commands.	?, page 1-5
arp	—	Display/manipulate/store the arp table.	arp, page 1-7
date	—	Set/show date.	date, page 1-9
diskusage	—	Display percentage of disk used.	diskusage, page 1-10
dns	Admin > System Setup > Configuration Information	Add/remove/show domain name resolving servers.	dns, page 1-11
dnssuffix	Admin > System Setup > Configuration Information	Add/remove/show domain name suffixes search path.	dnssuffix, page 1-12
domainname	—	Set/show name of the domain to which the MARS Appliance belongs.	domainname, page 1-13
ethtool	—	Display or change settings on an ethernet device.	ethtool, page 1-14
exit	—	Switch to standard mode/log out.	exit, page 1-17
expert	—	Switch to expert debugging mode (for using Cisco TAC personnel only).	expert, page 1-18
fips	—	Intializes the CS-MARS FIPS PCI Card	fips, page 1-19

Table 1-1 Command Summary (continued)

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
gateway	Admin > System Setup > Configuration Information	Show/set default gateway of the MARS Appliance.	gateway, page 1-22
help	—	Print list of available commands.	help, page 1-23
hostname	The *Name* field on the Admin > System Setup > Configuration Information page.	Set/show the hostname of the MARS Appliance.	hostname, page 1-25
hotswap	—	Hot add or remove hard disk drive.	hotswap, page 1-26
ifconfig	Admin > System Setup > Configuration Information	Configure/store network interface.	ifconfig, page 1-29
model	—	Displays the model number and mode of the MARS Appliance.	model, page 1-30
netstat	—	Show network statistics.	netstat, page 1-31
nslookup	—	Look up the IP address or domain name.	nslookup, page 1-32
ntp	—	Synchronize system clock with Network Time Protocol (NTP) servers.	ntp, page 1-33
passwd	Admin > User Management (pnadmin)	Change administrative password used to access the appliance from the Secure Shell (SSH) or GUI client.	passwd, page 1-35
passwd expert	—	Change the customer portion of the expert debugging mode password used to access the appliance from the Secure Shell (SSH).	passwd expert, page 1-36
ping	—	Sends Internet Control Message Protocol (ICMP) echo_request packets for diagnosing basic network connectivity.	ping, page 1-37
pndbusage	—	Shows the current database usage and explains how future space will be claimed, either through unused partitions or purging of oldest data.	pndbusage, page 1-39
pnexp	—	Export configuration and event data from a 4.3.x appliance for import into a MARS Appliance running 5.3.1 or later.	pnexp, page 1-40
pnimp	—	Import configuration and event data previously exported from a MARS Appliance running 4.3.x into a one running 5.3.1 or later.	pnimp, page 1-44

Table 1-1 Command Summary (continued)

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
pnlog	Admin > System Maintenance > View Log Files Admin > System Maintenance > Set Runtime Logging Levels Help > Feedback	Show system log/set log level.	pnlog show, page 1-53
pnreset	—	Reset the MARS Appliance to factory defaults.	pnreset, page 1-54
pnrestore	—	Restore MARS system configuration and data from a backup.	pnrestore, page 1-57
pnsshfs	Admin > System Parameters > SSL/SSH Settings	Handle outdated SSH keys	pnsshfs, page 1-61
pnstart	—	Start MARS applications.	pnstart, page 1-62
pnstatus	—	Show running status of MARS applications.	pnstatus, page 1-63
pnstop	—	Stop MARS applications.	pnstop, page 1-64
pnupgrade	Admin > System Maintenance > Upgrade Admin > System Parameters > Proxy Settings	Upgrade the software running on the MARS Appliance.	pnupgrade, page 1-65
predictfsck			
raidstatus[1]	—	Display the status of hard disk drives.	raidstatus, page 1-71
reboot	—	Reboot the MARS Appliance.	reboot, page 1-77
route	—	Configure/store routing tables.	route, page 1-78
script	—	Command line interface to provided script files. usage: script [-b] program	script, page 1-80
show healthinfo	—	Displays operational status of components in the MARS Appliance.	show healthinfo, page 1-81
show inventory	—	Displays identifying details of essential components in the MARS Appliance.	show inventory, page 1-83
shutdown	—	Shut down the MARS Appliance.	shutdown, page 1-85
snmpwalk	—	Communicates with a network entity using SNMP GETNEXT requests.	snmpwalk, page 1-86
ssh	—	User interface to the SSH client.	ssh, page 1-88
sslcert	—	Generate a new self-signed SSL certificate.	sslcert, page 1-90
ssllist	—	List existing ssl certificates	ssllist, page 1-91

Table 1-1 Command Summary (continued)

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
syslogrelay setcollector	—	Displays the IP address of the device to which syslogs are forwarded.	syslogrelay setcollector, page 1-92
syslogrelay src	—	Displays list of source addresses for which syslogs are forwarded.	syslogrelay src, page 1-93
syslogrelay list	—	Displays list of syslog collector and sources.	syslogrelay list, page 1-95
sysstatus	—	User interface to the Unix top command.	sysstatus, page 1-96
tcpdump	—	Dump traffic on a network.	tcpdump, page 1-98
telnet	—	User interface to the TELNET client.	telnet, page 1-99
time	—	Set/show time for the MARS Appliance.	time, page 1-100
timezone	—	Set/show timezone for the MARS Appliance.	timezone, page 1-101
traceroute	—	Displays the network route that packets take to reach a specified host.	traceroute, page 1-104
unlock	Admin > Management > User Management	Unlocks access to the GUI for all or specified accounts after login failure.	unlock, page 1-106
version	Help > About	Displays the version of software running on the MARS Appliance.	version, page 1-107

Commands

This section describes the Cisco Security Monitoring, Analysis, and Response System commands. Command names are case sensitive.

?

Use the **?** command to list available commands and command syntax.

?

Syntax Description

This command has no arguments or keywords.

Examples

The following example displays all available commands and their brief descriptions:

```
[pnadmin]$ ?
Commands are:
?                 - Print list of available commands
arp               - Display/manipulate/store the arp table
date              - Set/show date
diskusage         - Report filesystem disk space usage
dns               - Add/remove/show domain name resolving servers
dnssuffix         - Add/remove/show domain name suffixes search path
domainname        - Set/show domain name
exit              - Switch to standard mode/Logout
gateway           - Show/set default gateway
help              - Print list of available commands
hostname          - Set/show host name
hotswap           - hot add or remove disk
ifconfig          - Configure/store network interface
model             - Display the model info of CS-MARS
netstat           - Show network statistics
nslookup          - Look up the IP address or domain name
ntp               - Synchronize system clock with ntp servers
passwd            - Change password
ping              - Ping a host
pnimp             - Import Gen-1 box's configuration and events into this MARS
pnexp             - Export database content including configuration, events
pnlog             - Show system log/ set log level
pndbusage         - Show database usage info
pnreset           - reset the whole box to factory defaults
pnrestore         - restore system configuration and data
pnstart           - Start CS-MARS applications
pnstatus          - Show running status of CS-MARS applications
pnstop            - Stop CS-MARS applications
pnupgrade         - System upgrade
raidstatus        - Display the status of disks
reboot            - Reboot System
route             - Configure/store routing tables
show              - Show inventory and health monitoring information
shutdown          - Shutdown system
--More--(72%)
```

<snip>

The following example displays the syntax of the **unlock** command:

```
[pnadmin]$ unlock ?
Usage:
        unlock -a
        unlock {-l|-g|-b} user
```

Related Commands

Command	Description
help	Displays brief description of specified command
-h	Many commands support the -h keyword (a.k.a. option) to display syntax usage

arp

The **arp** command relates to the ARP cache on the MARS Appliance. You can view the list of mappings, clear an entry, or add a new mapping.

To display the current entries in the ARP cache, enter:

arp

To display the cached entries for a specific host, enter:

arp [**-evn**] [**-H** *type*] [**-i** *if_local*] **-a** [*hostname*]

To add a host to the cache, enter one of the following commands:

arp [**-v**] [**-H** *type*] [**-i** *if_local*] **-s** *hostname hw_addr* [*netmask*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if_local*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if_loca*] **-Ds** *hostname if_dest* [*netmask*] **pub**

To delete a host from the cache, enter:

arp [**-v**] [**-i** *if_local*] **-d** *hostname* [**pub** | **nopub**]

Syntax Description

no keyword, options, or arguments	Displays the IP address, hardware type, interface name, and MAC address associated with the network interface in the MARS Appliance.
-H *type*	When setting or reading the ARP cache, this optional parameter identifies which class of entries (hardware type) ARP should check for. The default value of this parameter is *ether*. The list of valid type values is as follows: • strip (Metricom Starmode IP) • ash (Ash) • ether (Ethernet) • tr (16/4 Mbps Token Ring) • tr (16/4 Mbps Token Ring [New]) • ax25 (AMPR AX.25) • netrom (AMPR NET/ROM) • rose (AMPR ROSE) • arcnet (ARCnet) • dlci (Frame Relay DLCI) • fddi (Fiber Distributed Data Interface) • hippi (HIPPI) • irda (IrLAP) • x25 (generic X.25)
-v	Tell the user what is going on by being verbose.
-n	Display numerical addresses instead of symbolic host, port, or usernames.

-a [*hostname*]	Displays the entries of the specified hosts. If the hostname parameter is not used, all entries are displayed.
-d *hostname*	Delete any entry for the specified host.
-D	Use the interface *if_dest*'s hardware address.
-e	Shows the entries in default (Linux) style.
-i *If_local*	Select an interface in the appliance. When dumping the ARP cache only entries matching the specified interface are printed. When setting a permanent or temp ARP entry, the entry is associated with this interface; if this option is not used, the routing table is used to determine the most likely interface through which the address is reachable. For *pub* entries the specified interface is the interface on which ARP requests are answered. This value must be different from the interface to which the IP datagrams will be routed (*if_dest*).
-**s** *hostname hw_addr*	Manually create an ARP address mapping entry for host hostname with hardware address set to *hw_addr* class. For the Ethernet class, use the 6-bytes in hexadecimal notation, separated by colons. You can determine this value using the **ipconfig /all** command on the host for which you are defining this entry. When adding proxy arp entries (that is, those with the publish flag set), a netmask may be specified to proxy arp for entire subnets. If the temp flag is not supplied entries are permanently stored in the ARP cache. You cannot define an ARP entry for an entire subnet.

Usage Guidelines

In all places where a hostname is expected, you can alternatively enter an IP address in dotted-decimal notation.

As a special case for compatibility the order of the hostname and the hardware address can be exchanged.

Each complete entry in the ARP cache is marked with the C flag. Permanent entries are marked with M and published entries have the P flag.

Note You cannot add arp entries from a file, as you do not have access to the file system on the MARS Appliance.

Examples

To permanently add an arp cache entry for a management host (marsgui) reachable from eth1, enter:

```
arp -v -H ether -i eth1 -s marsgui 00:05:9A:3C:78:00 pub
```

To remove the entry defined above, enter:

```
arp -v i eth1 -d marsgui nopub
```

date

To display or set the system date, use the **date** command.

date [*newdate*]

Syntax Description

no keyword	Default. Displays the date in the mm/dd/yy format (for example, 04/28/08)
newdate	Sets the MARS clock date in the format mm/dd/yyyy or mm/dd/yy.

Usage Guidelines

Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than 30 minutes, you should restart your appliance to ensure that all processes synchronize using the new time.

Examples

The following example displays the current date:

```
[pnadmin]$ date
06/25/07
```

The following example changes the current date to March 12, 2008:

```
[pnadmin]$ date 03/12/2008
[pnadmin]$ date
03/12/2008
```

diskusage

To display the disk space available on all partitions, use the **diskusage** command.

diskusage

Syntax Description

There are no keywords, options, or arguments.

Usage Guidelines

Displays amount of disk space available on all partitions in the MARS Appliance

For all MARS Appliance models, the Oracle database has three partitions:

- /u01: Stores the Oracle binary files.
- /u02: Stores the data files.
- /u03: Stores the replay log files, which are cached, in-memory working files not yet committed to the data store.

If any of these partitions reaches 99% capacity, the Oracle database will experience operational issues.

The size of the data partition (/u02) varies based on the model:

- MARS 20:   74 GB
- MARS 50: 148 GB
- MARS 100: 565 GB
- MARS 200: 795 GB

Examples

To display the disk usage for all partitions in the MARS Appliance, enter the following command:

```
diskusage
```

The following is sample output for a MARS 100, as noted by the size of the /u02 partition:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              20G  5.7G   13G  31% /
/dev/sda1             129M   14M  108M  12% /boot
/dev/sda5              20G  4.8G   13G  26% /opt
/dev/sda6              20G  130M   18G   1% /log
/dev/sda7              29G  134M   27G   1% /pnarchive
/dev/sda8              20G  2.7G   16G  14% /u01
/dev/sda9             9.8G  2.2G  7.2G  23% /u03
/dev/sda10            565G   15G  522G   3% /u02
none                 1005M     0 1005M   0% /dev/shm
```

dns

To display or specify the IP addresses of the Domain Name Services (DNS) servers that the MARS Appliance should use to resolve IP addresses into hostnames, use the **dns** command.

dns [*primary*] [*secondary*] [*tertiary*]

Syntax Description.

no keyword	The default behavior *of this command* displays the current set of IP addresses assigned to the primary, secondary, and tertiary DNS servers.
primary	Identifies the IP address of the DNS server that should be used first to resolve hostnames and/or IP addresses. Only the primary is required.
secondary	Identifies the IP address of the DNS server that should be used second to resolve hostnames and/or IP addresses. This address is optional. If this value is left blank, any previously defined secondary entries are deleted.
tertiary	Identifies the IP address of the DNS server that should be used last to resolve hostnames and/or IP addresses. This address is optional. If this value is left blank, any previously defined tertiary entries are deleted.

Usage Guidelines

If the DNS configuration is changed from the web interface, you must perform a pnstop and then a pnstart operation for the new DNS information to be used by the MARS Appliance. For information on performing these two operations, see Stop Appliance Services via the Console and Start Appliance Services via the Console in the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X*

Examples

The following example displays the current DNS server entries:

```
[pnadmin]$ dns
Primary DNS :   10.1.1.1
Secondary DNS :
Tertiary DNS :
```

The following example sets the primary DNS server to 192.168.101.3 and the secondary DNS server to 192.168.102.5, enter:

```
[pnadmin]$ dns 192.168.101.3 192.168.102.5
[pnadmin]$ dns
Primary DNS :192.168.101.3
Secondary DNS :192.168.102.5
Tertiary DNS :
```

The following example removes the secondary DNS server set in the previous example (192.168.102.5):

```
[pnadmin]$ dns 192.168.101.3
[pnadmin]$ dns
Primary DNS : 192.168.101.3
Secondary DNS :
Tertiary DNS :
```

dnssuffix

To display, add, or remove the DNS search paths associated with the adapters in the MARS Appliance, use the **dnssuffix** command.

dnssuffix [**add** | **del**] *searchpath*

Syntax Description

no keyword	The default behavior of this command displays the current domain search paths defined for the appliance.
add	Specifies that the text that follows “add” should be added as a new dns search path.
del	Specifies that the text that follows “del” should be removed from the dns search path, if found.
searchpath	Identifies the domain name to be used for local DNS searches.

Examples

To display the current DNS search path, enter:

```
dnssuffix
```

To add example.com to the search path, enter:

```
dnssuffix add example.com
```

To remove example.com from the search path, enter:

```
dnssuffix del example.com
```

domainname

To set or show the DNS domain of the MARS Appliance, use the **domainname** command.

domainname [*domain*]

Syntax Description

no keyword	Displays the current domain value if defined. Otherwise, it returns a blank line.
domain	Sets the MARS domain name to the specifed *domain* value.

Examples

To display the current domain name, enter:

```
domainname
```

The following command sets the domain name to example.com:

```
domainname example.com
```

ethtool

Use the **ethtool** command to display or change settings on an ethernet device.

ethtool [**option_letter**] {**eth*X***} **[option_parameters]**

where *X* is the number of the ethernet port (For example, eth0 or eth1).

Command History

Release	Modification
6.0.3	This command was introduced.

Syntax Description

[eth*X*]	Prints current setting of the specified device
-h	Shows a short help message
-a	Queries the specified ethernet device for pause parameter information
-A	Change the pause parameters of the specified ethernet device
autoneg on off	Specify whether pause autonegotiation is enabled
rx on off	Specify whether RX pause is enabled
tx on off	Specify whether TX pause is enabled
-c	Queries the specified ethernet device for for coalescing information
-C	Change the coalescing settings of the specified ethernet device
-g	Queries the specified ethernet device for for rx/tx ring parameter information
-G	Change rx/tx ring parameters of the specified ethernet device
rx *N*	Change number of ring entries for the Rx ring
rx-mini *N*	Change number of ring entries for the Rx Mini ring
rx-jumbo *N*	Change number of ring entries for the Rx Jumbo ring
tx *N*	Change number of ring entries for the Tx ring
-i	Queries the specified ethernet device for associated driver information
-d	Retrieves and prints a register dump for the specified ethernet device. When raw is enabled, then it dumps the raw register data to stdout.
-e	Retrieves and prints an EEPROM dump for the specified ethernet device
-E	Changes EEPROM byte for the specified ethernet device
-k	Queries the specified ethernet device for offload information
-K	Changes the offload parameters for the specified ethernet device
rx on off	Specify whether RX checksumming is enabled
tx on off	Specify whether TX checksumming is enabled

sg on off	Specify whether scatter-gather is enabled
-p	Initiates adapter-specific action intended to enable an operator to easily identify the adapter by sight. Typically this involves blinking one or more LEDs on the specific ethernet port.
N	Length of time to perform phys-id, in seconds
-r	Restarts auto-negotiation on the specified ethernet device, if auto-negotiation is enabled
-S	Queries the specified ethernet device for NIC- and driver-specific statistics
-t	Executes adapter selftest on the specified ethernet device. Possible test modes are **offline|online:** • **offline** (default) means to perform full set of tests possibly causing normal operation interruption during the tests • **online** means to perform limited set of tests that do not interrupt normal adapter operation
-s	option allows changing some or all settings of the specified ethernet device. All following options only apply if -s was specified
speed 10 | 100 | 1000	Set speed in Mb/s. ethtool with single argument will display the supported device speeds.
duplex half full	Set full or half duplex mode
port tp aui bnc mii fibre	Select device port
autoneg on off	Specify whether autonegotiation is enabled. (Typically it is on, but may be turned off to avoid problems with specific network devices.)
phyad *N*	PHY address
xcvr internal external	Select transceiver type.
wol p u m b a g s d	Set Wake-on-LAN options. Not all devices support this. The argument to this option is a string of characters specifying which options to enable: • **p** Wake on phy activity • **u** Wake on unicast messages • **m** Wake on multicast messages • **b** Wake on broadcast messages • **a** Wake on ARP • **g** Wake on MagicPacket (tm) • **s** Enable SecureOn (tm) password for MagicPacket (tm) • **d** Disable (wake on nothing). This option clears all previous options.
sopass %x:%y:%z:%a:%b:%c	Set the SecureOn (tm) password. The argument to this option must be six bytes in ethernet MAC hex format (xx:yy:zz:aa:bb:cc).
msglvl %d	Set the driver message level. Meanings differ per driver

Usage Guidelines

Enter **ethtool** without keywords or options to see the listing of supported parameters on MARS.

Examples

The following example displays the current parameters of the MARS Ethernet interface 0 (eth0):

```
[pnadmin]$ ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: umbg
        Wake-on: g
        Current message level: 0x00000007 (7)
        Link detected: yes
[pnadmin]$
```

The following example sets eth0 to 100 Mb/s, full duplex, with no autonegotiation:

```
ethtool -s eth0 speed 100 duplex full autoneg off
```

Related Commands

Command	Description
ifconfig	Displays or modifys the current IP address and network mask pairs associated with the network interfaces installed in the MARS Appliance.
show healthinfo	Displays the operational status of key components in the MARS appliance, including the Ethernet port numbers and their operational status.

exit

To log out of the system, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Examples

The following command logs you out of the system:

```
exit
```

expert

To enable expert debugging mode on the MARS Appliance, use the **expert** command.

expert

Syntax Description

There are no keywords, options, or arguments.

Usage Guidelines

This command prompts the user to provide authentication credentials to enable the expert debugging mode. Only authorized Cisco support personnel can properly authenticate.

The **expert** command, undocumented before the 4.1.3, is for exclusive use by Cisco to aid in debugging customer issues that require direct access to the internal data store of the MARS Appliance. You may further restrict access to the **expert** command by setting the customer portion of the expert mode password via the **passwd expert** command. This command removes the default expert mode password set on the appliance from the factory.

While you can use the **passwd expert** command to restrict access to the **expert** command, only authorized Cisco support personnel are able to access the expert debugging mode of an appliance.

Examples

The following example

```
[pnadmin]$ expert
Password:
```

Related Commands

Command	Description
passwd expert	Changes the customer portion of the password associated with expert debugging mode of the appliance,

fips

To intialize, zeroize, or to check the status of the CS-MARS FIPS PCI Card, use the **fips** command.

fips [init | zeroize | status]

Command History

Release	Modification
6.0.5	This command was introduced for the CS-MARS-110R-K9.

Syntax Description

init	Initializes the FIPS PCI Card and supporting software.
zeroize	Destroys the cryptographic key created with the **fips init** command such that the key cannot be recovered by any means.
status	Displays the status of the FIPS PCI Card and its supporting software.

Usage Guidelines

The **fips** command is active only for the CS-MARS 110R appliance equipped with the CS-MARS FIPS PCI Card.

Use the **fips init** command to activate the FIPS PCI Card, after which all cryptographic functions normally performed by the MARS operating system for Java security, SSH, SSL and TLS are offloaded to the FIPS PCI Card. The tamper-evident coating on the FIPS PCI Card, its encryption algorithms, and its security methods, conform to United States Government Federal Information Processing Standard FIPS 140-2 Level 2. The initialization process requires that three Smart Cards be initialized too, but the Smart Cards are not used in any subsequent MARS operations. After FIPS initialization, the MARS operates exactly as before, but with the following exceptions:

- The CS-MARS model number changes from CS-MARS-110R to CS-MARS-110RF
- With the FIPS PCI Card initialized, you must reboot the CS-MARS 110RF after executing a **sslcert** command.
- A Global Controller cannot parse information received from a CS-MARS-110RF

To manually destroy the FIPS cryptographic keys on the FIPS PCI Card, use the **fips zeroize** command. The zeroize option forces a reboot, and restablishes standard MARS encryptions. The zeroize option makes recovery of the FIP cryptographic keys impossible. After issuing a **fips zeroize** command, you must reinitialize the FIPS PCI Card to generate new FIPS keys and to reestablish FIPS 140-2 Level 2 security. The ability to manually destroy the cryptographic keys is a FIPS requirement. A **fips init** command zeroizes the FIPS PCI Card as part of the initialization process.

Use the **fips status** command to display the current operating status and version numbers of the FIPS PCI Card and its supporting software. The “Module #1” section refers to the physical FIPS PCI Card. The “Server” section refers to software that controls communication between MARS applications and the FIPS PCI Card. The server runs as a daemon on MARS. The FIPS security is in place when both the server and module (FIPS PCI Card) modes are operational. For more information on the CS-MARS FIPS PCI Card, see the ***CS-MARS FIPS PCI CARD Quick Install*** document at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/fru/fipsfru.html

Use the **show inventory** command to verify that the FIPS PCI Card is physically installed. Use the **model** command to verify that the FIPS PCI Card is initialized (It is initialized when the model is CS-MARS-100RF).

Examples

The following **show inventory** command example verifies that the FIPS PCI Card is installed.

```
[pnadmin]$ show inventory
NAME: "Chassis",  DESCR: "CS-MARS-110 Local Controller"
PID: CS-MARS-110,       VID: V01,       SN: M1100000011

FIPS HSM: nCipher nShield 500e,          SN: 4F06-81E7-8838

<snip>
```

The following **model** command example shows the MARS model number as CS-MARS-110RF after intialization of the FIPS PCI Card (changed from model CS-MARS-110R):

```
[pnadmin]$ model
CS-MARS-110RF
```

The following example shows the output of **fips status** command.

```
[pnadmin]$ fips status
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        4F06-81E7-8838
 mode                 operational
 version              2.36.16
 speed index          544
 rec. queue           442..642
 level one flags      Hardware HasTokens
 version string       2.36.16cam12, 2.33.82cam1 built on Mar 06 2008 15:55:03
 checked in           00000000482ab2dd Wed May 14 02:37:33 2008
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004

Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        4F06-81E7-8838
 mode                 operational
 version              2.33.82
 speed index          544
 rec. queue           9..152
 level one flags      Hardware HasTokens
 version string       2.33.82cam1 built on Mar 06 2008 15:55:03
 checked in           0000000047d0118d Thu Mar  6 07:45:17 2008
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard
 module type code     7
 product name         nC1003P/nC3023P/nC3033P
 device name          #1 nFast PCI device, bus 12, slot 0.
 EnquirySix version   5
 impath kx groups     DHPrime1024
 feature ctrl flags   LongTerm
 features enabled     StandardKM
 version serial       24
 rec. LongJobs queue  8
 SEE machine type     PowerPCSXF
```

Related Commands

Command	Description
model	Displays the model name of the MARS Appliance.
show inventory	Displays identifying details of essential components in the appliance (such as an installed FIPS PCI Card).
sslcert	Generates a new self-signed SSL certificate and reboots the JBoss Application Server.

gateway

To show or set the default gateway to be used by the MARS Appliance, use the **gateway** command.

gateway [*address*]

Syntax Description

no keyword	Displays the current gateway setting, if defined. Otherwise, it displays no value.
address	Changes the default gateway address to the specified value. Use decimal notation.

Examples

To display the current default gateway address used by the appliance, enter:

```
gateway
```

To set the default gateway address to 192.168.101.1, enter:

```
gateway 192.168.101.1
```

help

The **help** command displays a complete list of commands that are available at the serial console.

help [*name]*

Usage Guidelines

no keyword	Displays the full list of commands that are available and their corresponding brief description.
name	Identifies the command for which you want to see the brief description.

Examples

The following example displays a list of available commands:

```
[pnadmin]$ ?
Commands are:
?                 - Print list of available commands
arp               - Display/manipulate/store the arp table
date              - Set/show date
diskusage         - Report filesystem disk space usage
dns               - Add/remove/show domain name resolving servers
dnssuffix         - Add/remove/show domain name suffixes search path
domainname        - Set/show domain name
exit              - Switch to standard mode/Logout
gateway           - Show/set default gateway
help              - Print list of available commands
hostname          - Set/show host name
hotswap           - hot add or remove disk
ifconfig          - Configure/store network interface
model             - Display the model info of CS-MARS
netstat           - Show network statistics
nslookup          - Look up the IP address or domain name
ntp               - Synchronize system clock with ntp servers
passwd            - Change password
ping              - Ping a host
pnimp             - Import Gen-1 box's configuration and events into this MARS
pnexp             - Export database content including configuration, events
pnlog             - Show system log/ set log level
pndbusage         - Show database usage info
pnreset           - reset the whole box to factory defaults
pnrestore         - restore system configuration and data
pnstart           - Start CS-MARS applications
pnstatus          - Show running status of CS-MARS applications
pnstop            - Stop CS-MARS applications
pnupgrade         - System upgrade
raidstatus        - Display the status of disks
reboot            - Reboot System
route             - Configure/store routing tables
show              - Show inventory and health monitoring information
shutdown          - Shutdown system
--More--(72%)
```

<snip>

The following example displays just the brief description of the **netstat** command:

```
[pnadmin]$ help netstat
Commands are:
netstat           - Show network statistics
```

Related Commands

Command	Description
?	Displays a complete list of available commands or usage of specific commands
-h	Many commands support the -h keyword (a.k.a. option) to display syntax usage

hostname

To set or show the hostname of the MARS Appliance, use the set **hostname** command.

hostname [*hostname*]

Syntax Description

no keyword	Displays the current hostname value, if defined. Otherwise, it displays no value.
hostname	Identifies the value to which the hostname for the MARS Appliance should be set.

Usage Guidelines

Changing the hostname requires that the appliance reboot. This reboot will occur automatically after your change the hostname. However, you are prompted to verify the hostname change. To cancel the hostname change without rebooting, enter **no** at the `Hostname change will cause the system to reboot. Do you want to proceed?` prompt.

Examples

This command sets the MARS Appliance name to csmars1:

```
hostname csmars1
```

To see the current hostname, enter:

```
hostname
```

hotswap

Use the **hotswap** command to remove and add hard drives to MARS Appliances with RAID arrays and to determine the physical layout of the hard drives. A **hotswap remove** and **add** command sequence *must* be executed before a hard drive is physically removed from or added to the RAID array.

hotswap list all

hotswap{**add** | **remove**} *disk*

Command History

Release	Modification
3.X	This command was introduced.
5.2.4	The **list all** keyword was added. The *disk* argument range of values include 0.
5.3.2	The **list all** keyword was modified to display the chassis hard drive slot to Port and PD number map; support for MARS 55 was added.

Syntax Description

list all	Displays a map of chassis hard drive slots and their related Port or PD number.
add	Indicates that the hard drive with the designated *disk* number is to be added to the RAID array.
remove	Indicates that the hard drive with the designated *disk* number is to be removed from the RAID array.
disk	Thechassis hard drive slot number of the hard drive to be hotswapped.

Usage Guidelines

To hotswap a hard drive is to replace the hard drive without powering down or rebooting the appliance.

For MARS Appliances 100, 100E, 200, GCM, and GC, the valid *disk* arguments range from 1 to 8.

For MARS Appliances 110, 110R, 210, GC2R, and GC2, the valid *disk* arguments range from 0 to 5.

For the MARS Appliance 55 the valid *disk* arguments are 0 and 1.

To hotswap a hard drive, execute **hotswap remove** *disk*, replace the hard drive in the slot designated by *disk*, then execute **hotswap add** *disk*. Check the operational status of the hard drive and the RAID array with the **raidstatus** command.

Whenever a **hotswap remove** *disk* command is executed, the hard drive in that slot is removed from the array and another must be added to restore full redundancy to the RAID array.

If the wrong *disk* value is entered, that hard drive is dropped from the RAID array, but can be rebuilt into the array without physically removing and inserting the hard drive by executing a **hotswap add** *disk* command. It can take up to 300 minutes for a single hard drive to be rebuilt into the RAID array.

For more information on RAID hotswapping procedures, see the chapter, “System Maintenance” in the *User Guide for Cisco Security MARS Local Controller* at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/local_controller/maintain.html

Examples

In the following example, a hard drive is hotswapped in slot 5 of a MARS 210. The hard drive status is verified with the **raidstatus** command:

```
[pnadmin]$ version
5.3.2 (2702)
[pnadmin]$ hotswap list all
Hardware RAID is found with 6 disks!
Disks available to be hotswapped:
        |==============|==============|==============|
        |     PD 1     |     PD 3     |     PD 5     |
        |--------------|--------------|--------------|
        |     PD 0     |     PD 2     |     PD 4     |
        |==============|==============|==============|

[pnadmin]$ hotswap remove 5

Adapter: 0: EnclId-14 SlotId-5 state changed to OffLine.
Disk 5 can now be safely removed from the system.


[pnadmin]$ raidstatus
Adapter Information:
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version : 1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size            Cache
---------------------------------------------------------------
a0      Raid-10         Degraded        64kB    2097151MB       Enabled

PD      Status  Size & Block                            Model
        Serial#
--------------------------------------------------------------------------------
p0      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EEZ
p1      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09CQT
p2      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD094KY
p3      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD08NZX
p4      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EWP
p5      Offline 715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD06AQ2


[pnadmin]$ hotswap add 5

Started rebuild progress on device(Encl-14 Slot-5)
Disk 5 has been successfully added to RAID



[pnadmin]$ raidstatus
Adapter Information:
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version :  1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size            Cache
---------------------------------------------------------------
a0      Raid-10         Degraded        64kB    2097151MB       Enabled

PD      Status  Size & Block                            Model
```

```
        Serial#
--------------------------------------------------------------------------------
p0      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EEZ
p1      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09CQT
p2      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD094KY
p3      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD08NZX
p4      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EWP
p5      Rebuild 715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD06AQ2

Rebuild Progress on Device at Enclosure 14, Slot 5 Completed 17% in 32 Minutes.
```

Related Commands

Command	Description
raidstatus	Displays the status of the RAID array and of the individual HDDs.
show inventory	Displays information on chassis, hard drives and power supplies

ifconfig

To display or modify the current IP address and network mask pairs associated with the network interfaces installed in the MARS Appliance, use the **ifconfig** command.

ifconfig {**eth0** | **eth1**} *ip_address netmask*

Syntax Description

no keyword	Displays the current settings for both the eth0 and eth1 interfaces.
eth0	Identifies that you want to set the IP address/netmask value for the eth0 interface. This option cannot be used in conjunction with eth1. If you do not specify the *ip_addr* and `netmask` values, this option displays the current settings for the eth0 interface.
eth1	Identifies that you want to set the IP address/netmask value for the eth0 interface. This option cannot be used in conjunction with eth0. If you do not specify the *ip_addr* and `netmask` values, this option displays the current settings for the eth1 interface.
ip_address	Specifies the IP address to assign to the specified interface (eth0 or eth1). You must specify a netmask value following this value.
netmask	Identifies the network mask value to use with the address specified. You must specify the IP address before specifying this value.

Usage Guidelines

For more information on the physical placement of eth0 versus eth1, see the corresponding appliance model under Physical Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2 or Physical Descriptions—MARS 20R, 20, 50, 100E, 200, GCm, and GC, in the Cisco Security MARS Hardware Installation and Maintenance Guide, 6.X.

For MARS Appliances 110, 110R, 210, GC2R, and GC2, eth0 is the integrated NIC 1, eth1 is the integrated NIC 2; eth2 and eth4 are unsupported.

Examples

To display the current interface address settings, enter:

```
ifconfig
```

To set the IP address of eth1 to 192.168.101.2/32, enter:

```
ifconfig eth1 192.168.101.2 255.255.255.255
```

Related Commands

Command	**Description**
show healthinfo	Displays operational status of appliance components.

model

Use the **model** command to display the model name of the MARS Appliance.

model

Syntax Description

There are no keywords

Examples

The following displays the model information about the MARS Appliance:

```
[pnadmin]$ model
mars50
local
standard
[pnadmin]$
```

netstat

Use the **netstat** commands to display the status of network connections on either TCP, UDP, RAW or UNIX sockets.

netstat [-h] [-r] [-v] [-V]

Syntax Description

no option	The default behavior of this command lists current Internet connections and UNIX domain sockets.
-h	Displays the detailed usage guidelines on this command
-r	Displays information about the routing table on the MARS Appliance.
-v	Displays verbose information. Useful for obtaining information about unconfigured address families.
-V	Displays version of command.

Usage Guidelines

By default, the **netstat** command only displays status on active sockets that are not in the LISTEN state (that is, connections to active processes).The MARS **netstat** command is a partial implementation of the LINUX version.

nslookup

Look up the IP address or domain name using its counterpart. This command launches an interactive console that displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works.

Syntax Description

nslookup puts you into interactive command mode. To quit the command mode and return to the command prompt, enter **exit**.

ntp

Use **ntp server** to identify the primary and secondary NTP server with which the appliance should synchronize. To force a synchronization with the NTP server, use **ntp sync**. To disable the use of ntp by this appliance, use **ntp disable**.

ntp server [*ntp_server1*] [*ntp_server2*]

ntp sync

ntp disable

Syntax Description

no keyword	Displays the current settings for the NTP servers. If no servers have been identified, it displays the message: ntp is not setup.
server	
ntp_server1	Identifies the server, by IP address, that runs the NTP server from which you want this MARS Appliance to retrieve system time information. This time value sets the clock used to date and correlate events that are received by the appliance.
ntp_server2	
sync	Forces the MARS Appliance to synchronize with the NTP server. If the first server is unreachable, the appliance attempts to synchronize with the secondary server.
disable	Disables the use of NTP on the MARS Appliance.

Usage Guidelines

The Network Time Protocol (NTP) synchronizes the clocks of computers across a network. By specifying an NTP server, you are instructing the appliance to contact that server to retrieve appropriate time settings. Synchronized times is especially important to MARS, because timestamp information provided by the reporting devices (and the appliance itself) is critical to accurate reconstruction of what transpires on the network.

Note Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than 30 minutes, you should restart your appliance to ensure that all processes synchronize using the new time.

Warning **When operating in a Global Controller/Local Controller hierarchy configuration, you must configure NTP on the Global Controller and on each Local Controller to ensure that rules fired by the Local Controller are properly propagated to the Global Controller.**

Examples

To specify that 192.168.101.5 and 192.168.103.21 are your primary and secondary NTP servers, respectively, enter:

```
ntp server 192.168.101.5 192.168.103.21
```

To force a synchronization between the MARS Appliance and the NTP servers you have identified, enter:

```
ntp sync
```

To disable NTP synchronization, enter:

```
ntp disable
```

Related Commands

Command	Description
time	Displays and configures the MARS timeclock
timezone	Displays and configures the MARS timezone setting

passwd

To change the password of the system administrative account (pnadmin) associated with the appliance, use the **passwd** command.

passwd [*new_pword*]

Syntax Description

no keyword	Generates a prompt to enter a new system administrative password.
new_pword	Generates a prompt to enter a new system administrative password.

Usage Guidelines

Examples

To change the system administrative account password to *Ou812o*, enter:

```
[pnadmin]$ passwd
New password: <Ou812o>
Retype new password: <Ou812o>
[pnadmin]$
```

passwd expert

To change the customer portion of the password associated with expert debugging mode of the appliance, use the **passwd expert** command.

passwd expert [*new_pword*]

While you can use the **passwd expert** command to restrict access to the **expert** command, only authorized Cisco support personnel are able to access the expert debugging mode of an appliance.

See also expert, page 1-18.

Syntax Description

no keyword	Begins change password dialog
new_pword	Sets the password to which you want to set the expert mode password.

Examples

To change the customer portion of the password associated with expert mode of the appliance to *Ou812o*, enter:

```
[pnadmin]$ passwd expert
New password: <Ou812o>
Retype new password: <Ou812o>
[pnadmin]$
```

Related Commands

Command	Description
expert	Enables expert debugging mode on the MARS Appliance

ping

To send ICMP echo_request packets for diagnosing basic network connectivity between the appliance and a network host, use the **ping** command.

ping [**-LRUbdnqrvV**] [**-c** *count*] [**-i** *interval*] [**-w** *wait*] [**-p** *pattern*] [**-s** *packetsize*] [**-t** *ttl*] [**-I** *if_addr*] [**-T** *option*] [**-Q** *tos*] *host*

Syntax Description

no keyword or option	The default behavior *of this command* displays the command's usage guidelines.
-b	Allow pinging a broadcast address.
-c *count*	Stop after sending count ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.
-d	Set the SO_DEBUG option on the socket being used.
-i *wait*	Identifies the wait interval in seconds between each sent packet. The default is one second.
-I *if_addr*	Set source address to the specified interface address.
-l *preload*	If preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior. Only the super-user can use this option.
-L	Suppress loopback of multicast packets. This flag only applies if the ping destination is a multicast address.
-n	Numeric output only. No attempt will be made to look up symbolic names for host addresses.
-p *pattern*	You can specify up to 16 "pad" bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, "-p ff" will cause the sent packet to be filled with all 1s.
-Q *tos*	Set Quality of Service-related bits in ICMP datagrams. The tos value can be either decimal or hex number. Traditionally (RFC1349), these have been interpreted as 0 for reserved (currently being redefined as congestion control), 1-4 for Type of Service, and 5-7 for Precendence. Possible settings for Type of Service are minimal cost, 0x02; reliability, 0x04; throughput, 0x08; and low delay, 0x10. Multiple TOS bits should not be set simultaneously. Possible settings for special Precedence range from priority (0x20) to net control (0xe0). You must be root (CAP_NET_ADMIN capability) to use Critical or higher Precedence value. You cannot set bit 0x01 (reserved) unless ECN has been enabled in the kernel. In RFC2474, these fields have been redefined as 8-bit Differentiated Services (DS), consisting of bits 0-1 of separate data (ECN will be used, here), and bits 2-7 of Differentiated Services Codepoint (DSCP).
-q	Quiet output. Nothing is displayed except the summary lines at startup time and when finished.
-R	Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.

-r	Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.
-s *packetsize*	Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
-t *ttl*	Set the IP Time to Live for multicasted packets. This flag only applies if the ping destination is a multicast address.
-T *option*	Set special IP timestamp options. Timestamp option may be either tsonly (only timestamps), tsandaddr (timestamps and addresses), or tsprespec host1 [host2 [host3 [host 4]]] (timestamp prespecified hops).
-M *hint*	Select Path MTU Discovery strategy. **hint** may be either do (prohibit fragmentation, even local one), want (do PMTU discovery, fragment locally when packet size is large), or don't (do not set DF flag).
-U	Print true user-to-user latency (the old behavior).
-v	Displays verbose output.
-V	Displays the version of this command.
-w *deadline*	Specify a timeout, in seconds, before ping exits regardless of how many packets have been sent or received.

Usage Guidelines

This is standard LINUX implementation of the PING command.

Use Ctrl+C or ^C to stop the output of this command and return to the command prompt.

Note The options used in this command are case sensitive.

pndbusage

To display the percentage of total storage space used by the database, use the **pndbusage** command:

pndbusage

Syntax Description

There are no keyword, options or arguments for this command.

Usage Guidelines

This command displays the percentage used within the current partition, as well as specifies whether additional partitions are available. If no unused partitions exist, the command identifies which partition will be purged, provides an approximate schedule for when that purge will occur, and specifies the date range and total number of events scheduled to be purged.

Examples

Two possible outputs exist for this command:

- If empty partitions are available, the output appears as follows:

```
Current partition started on <start date> and uses
<number>% of its available capacity.
Switching to next partition is estimated for <estimated switching date>
<number> empty partitions are available for storage.
```

- If no empty partitions exists, the output appears as follows:

```
Current partition started on <start date> and uses
<number>% of its available capacity.
Switching to next partition is estimated for <estimated switching date>
<number> events, received between <purge start date> and <purge end date> will be
purged.
```

In this case, the third line indicates the data that will be purged on the <estimated switching date>.

Indents are displayed as shown above.

pnexp

Use the **pnexp** configuration mode to determine the time and disk space requirements for a data export, to review the size of the database and the data characteristics, to start and stop the export of configuration data, event data, or both, and to check the status of an ongoing export. To access the **pnexp** configuration mode, enter the **pnexp** command at the `[pnadmin]$` prompt:

pnexp

Command History

Release	Modification
4.3.1	This command was introduced in the Local Controller and Global Controller version 4.x train.
4.3.4	Support for exporting to a SFTP server was added.
6.0.1	This command was implemented for all MARS hardware.

Syntax Description

help	Displays a list of valid subcommands.
quit | exit	Quit and exit the **pnexp** command. Return to the pnadmin command prompt.
status	Display the status of the current data export operation.
log {all | recent}	Show all or recent data exporting log entries.
data	Displays the number of events, report results, statistics, and incidents in the database.
config	Displays the number of devices, reports, and rules in the database. This command should be used as a point of comparison once the configuration is imported into the target appliance. Compare with the output of the **pnimp config** command.
stop	Stop the data export operation.

esti_time [MM/DD/YY:HH]

Estimates how much time and storage is required to export the event data that was received by MARS after a specified start time—only the events received after that time are migrated. If the last argument is not specified, then the estimate is based on all event data in the database.

Note The data export tool ignores data that was previously archived for the MARS Appliance. Each time the command is run, it writes data to a new NFS directory regardless whether data has already been archived.

export {config | data | all} {*nfs_path*} [MM/DD/YY:HH]

Export MARS configuration data ({**config**}), or events/reports/statistics/incidents data ({**data**}), or both ({**all**}) to the specified NFS or SFTP remote server path ({*remote-path*}). If the last optional argument is given, only data received after that time will be exported.

- Example export to NFS server:

```
export all 10.1.1.1:/mars/archive 02/28/07:00
```

The *remote-path* value identifies the IP address of the remote server plus the top-level archive folder on the remote server; it does not identify a specific archive date. The value format is [sftp:[<*username*>@]] *IP_address*:*FolderPath* . If sftp is not specified, a NFS server path is assumed.

- Example config only export to a NFS server:

```
export config 10.1.1.1:/archive
```

- Example data only export to a SFTP server:

```
export data sftp:10.1.1.1:/archive
```

If you export event data to an NFS server, the specified NFS path value must *not* match the archive path used by the source appliance. The **pnexp** command creates the proper archive folder under this path.

Note Only the start date is specified, the end date is always the current time (when event receiving is stopped).

Usage Guidelines

Use the **pnexp** command to prepare and export configuration and event data from a MARS Appliance running 4.x, or 5.x as separate data so you can import either or both on a MARS Appliance running 6.x software. When the export process begins, that MARS Appliance stops receiving events until the export process completes.

Caution Once the export process begins, event data published to this appliance is lost, as is any event data that is not already written to the database. To avoid losing event data, follow the instructions provided in the Migrating Data from Cisco Security MARS 4.x to 6.0.1 documentation, sections Same Appliance Data Migration Work Flow and Different Appliance Data Migration Work Flow.

Note The **export** process stops other software module processes on the MARS Appliance (see pnstatus). To restart the modules, reboot the MARS Appliance with the **reboot** command.

The configuration export runs in the foreground displaying its status and errors immediately, where as event data export runs in the background. Use the **log {all | recent}** command to view the running status log for event data export.

The event export part of this operation can take a long time, as the export speed ranges between 6,000 and 30,000 events per second depending on the appliance model. Event data is exported in the following order: report result, statistics, incident and firing events, and event session. If the remote NFS server becomes unavailable during a lengthy export operation, the **pnexp** program attempts to remount the server. For event data export, logs are written to the `/log/export.log` file.

To exit **pnexp** configuration mode, enter `exit` at the `pnexp>` prompt.

For detailed explanations on data export, import, and migration, see the document, *Migrating Data from Cisco Security MARS 4.x to 6.0.1*, at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/migration/guide/dmigrate6x.html

Examples

The following example specifies that the MARS Appliance should export the configuration data to the NFS archive found at 192.168.3.138:/storage/mars_migration:

```
pnexp> export config 192.168.3.138:/storage/mars_migration
WARNING: this will stop CS-MARS, do you wish to continue (yes/no): yes

!!! The exported config data is saved under sub-directory of
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
!!! Stopping CS-MARS processes ...
!!! Exporting config data now

Dumping configuration data, may take a while ...
Configuration dump finished.
Configdump to 192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10 finished
successfully.
```

The following example specifies that the MARS Appliance should export the event data corresponding to the configuration data in the previous example:

```
pnexp> export data 192.168.3.138:/storage/mars_migration 05/01/07:0
WARNING: this will stop CS-MARS, do you wish to continue (yes/no): yes

Estimated total number of events to export: 1401080357
Estimated time to export events: 12 hours 58 minutes
Estimated space for exported events: 66809 MB

Do you wish to continue (yes/no): yes
!!! The exported event data is saved at
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
!!! Stopping CS-MARS processes ...
!!! Restarting oracle ...
!!! Exporting data in background now, enter 'status' or 'log' to view data exporting
status and/or logs.
```

Tip Use the **log all** command to determine where the archives are saved. This path information is required by the **pnimp** command.

```
Sep  4 11:25:21.293 2007@LM_INFO@Thread 1024:START DATA EXPORTING...
Sep  4 11:25:21.293 2007@LM_INFO@Thread 1024:Parameter: nfs_path =
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
Sep  4 11:25:21.293 2007@LM_INFO@Thread 1024:Parameter: event_start_time = 05/01/07:0
Sep  4 11:25:21.395 2007@LM_INFO@Thread 1024:Trying to mount /mnt/pnarchive
Sep  4 11:25:22.677 2007@LM_INFO@Thread 1024:EXPORTING REPORT RESULTS ...
```

Related Commands

Command	Description
pnimp	Import configuration and event data into a MARS Appliance running version 5.3.1 or later.

pnimp

From the **pnimp** command prompt, you can access time required for a data import, review the size of the event data set on the NFS server, start and stop the import of configuration data or event data, and check the status of an ongoing import. To access the **pnimp** command prompt, use the **pnimp** command at the pnadmin prompt:

```
pnimp
```

Command History

Release	Modification
5.3.1	This command was introduced for the Local Controller and Global Controller operating Release 5.x
5.3.4	Support for importing from a SFTP server was added.
6.0.1	This command was implemented for all MARS hardware.

Syntax Description

help	Displays a list of valid subcommands.
quit | exit	Quit and exit the **pnimp** command. Return to the pnadmin command prompt.
status	Display the status of the current data import operation.
log {all | recent}	Show all or recent data import log entries.
data {*remote-path*}	Show how much data exists in the specified remote path, which is either a NFS or SFTP server.
config	Displays the number of devices, reports, and rules in the migration data set. This command should be used as a point of comparison after the configuration is imported into the target appliance. Compare with the output of the **pnexp config** command.
stop	Stop the data import operations.

esti_time {remote-path} {MM/DD/YY}

Estimates how much time is required to import the event, report, statistics, and incident data found at the specified remote path. The *MM/DD/YY* parameter restricts the estimate to data generated on or after that date.

Note This command does not estimate the time required to import configuration data.

import {config | data} {*remote-path*} [MM/DD/YY]

Import MARS configuration data ({config}), or events/reports/statistics/incident data ({data}) from the specified NFS or SFTP remote server path ({remote-path}). The last argument ([MM/DD/YY]) specifies the start date from which to begin importing events; all events from that date forward are imported. It is required for importing events/reports/statistics/incident data, meaning only importing data received or computed on or after that date. For importing config data, the latest MARS configuration data found under *remote-path* is used.

The *remote-path* value identifies the exported archive folder on the NFS or SFTP remote server; this path was dispayed when you ran the **pnexp export** command. The value format is [sftp:[<*username*>@]] *IP_address*:*FolderPath* . If sftp is not specified, a NFS server path is assumed.

Examples:

Example config only import from a NFS server:

```
import config 10.1.1.1:/archive
```

Example data only import from a SFTP server:

```
import data sftp:10.1.1.1:/archive
```

Note You must first import the corresponding configuration data before attempting to import the event, report, statistics, incident data for reporting devices.

Usage Guidelines

Use the **pnimp** command to import configuration and event data generated from a MARS Appliance running 4.3.6 or 5.x into a MARS Appliance running 6.x software. The import operation does not affect event processing; in other words, the received events are processed upon arrival. However, it does affect the web interface and the query and report features may experience long delays and missing event or session data.

Tip To avoid IP address conflicts, reconfigure the MARS Appliance running 4.x before you import its configuration data into a new appliance.

Note When you import configuration data, it overwrites the configuration running on the MARS Appliance and reboots the appliance. After rebooting, the MARS Appliance assumes the IP address, hostname, and username/password of the appliance from which the configuration archive was exported.

The configuration import runs in the foreground displaying its status and errors immediately, where as event data export runs in the background. Use the **log {all | recent}** command to view the running status log for event data import.

Recent data is imported first. If an NFS-related problem results in a file not being imported properly, the **pnimp import** program halts and logs an error to the `/log/migrationrestore.log` file.

The next time the import operation is started, you are prompted whether to retry the last failed file. If no, the import operation continues with the next file. If another problem occurs, for example, a file corruption, that prevents a file from being imported, **pnimp import** generates a log similar to "file es_334_...gz is imported with error!" and continue with the next file.

When the import operation completes, the Local Controller begins to rebuild the RAW message indices. You can use the web interface although keyword query will remain slow until the indices are rebuilt.

For detailed explanations on data export, import, and migration, see the document, *Migrating Data from Cisco Security MARS 4.x to 6.0.1*, at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/migration/guide/dmigrate6x.html

Examples

The following example specifies that the MARS Appliance should import the configuration data from the NFS archive found at 192.168.3.138/storage/mars_migration/:

```
[pnadmin]$ pnimp
Enter 'help' for a list of valid commands, 'exit' or 'quit' to exit.

pnimp> import config 192.168.3.138:/storage/mars_migration/LC-220_2008-09-04-11-25-10
09/04/07
The most recent configuration archive from 4.3.5 release or later found on the NFS server
was created at 2008-09-04-11-25-10. Because events received after the config archive was
created may not be imported correctly later on when you try to import event data, so if
possible, you should always use 'pnexp' to export a fresh copy of configuration from the
Gen-1 MARS box before trying this command.

Do you wish to continue (yes/no) : yes

WARNING: this operation will overwrite current MARS box's configurations (both system and
DB) and reboot the machine. After reboot, current MARS box will take over the IP address,
hostname and MARS username/password of the MARS box from which the config archive was
exported, please make sure there will be no IP address conflict.

Do you wish to continue (yes/no): yes
!!! Stopping CS-MARS processes …
Invoking binary config importing procedure …
Recreating the database schema.
Importing data into database …
Configuration data binary import done.
Configrestore succeeded!
!!! Updating system settings …
Broadcast message from root (pts/5) (Wed Jun 13 15:23:46 2008):

The system is going down for reboot NOW!
[pnadmin]$
```

The following example specifies that the MARS Appliance should import the event data corresponding to the configuration data in the previous example:

```
pnadmin]$ pnimp

Enter 'help' for a list of valid commands, 'exit' or 'quit' to exit.
pnimp> import data 192.168.3.138:/storage/mars_migration/LC-220_2008-09-04-11-25-10
01/01/07
```

```
Last imported configuration archive is from
192.168.3.138:/storage/mars_migration/LC-220_2008-09-04-11-25-10/2008-09-04/CF/cf-4318-431
_2008-09-04-11-25-10.pna created at 2008-09-04-11-25-10. Because events received after the
config archive was created may not be imported correctly, you should import a latest copy
of configuration from the Gen-1 MARS box before trying this command if possible.

Do you wish to continue (yes/no): yes
Total number of days with data : 5
Total number of event archives to import: 89
Total number of report result archives to import: 1
Total number of statistics archives to import: 4
Total number of incident archives to import: 3
Estimated time to import all events: 2 hours 1 minutes

Do you wish to continue (yes/no): yes
!!! Importing data in background now, enter 'status' or 'log' to view data importing
status and/or logs.

pnimp>
```

The following example displays the number of devices, reports, and rules in the migration data set. This command is run after the configuration is imported into the target appliance:

```
pnadmin]$ pnimp

Enter 'help' for a list of valid commands, 'exit' or 'quit' to exit.
pnimp> config
Num of devices: 42482
Num of interfaces: 51284
Num of networks: 86
Num of network groups: 3
Num of reports: 253
Num of report groups: 31
Num of rules: 1261
Num of rule groups: 16
Num of users: 30
Num of user groups: 5
```

Related Commands

Command	Description
pnexp	Export configuration and event data from a MARS Appliance running version 4.x (4.3.1 or later).

pnlog

To set the logging level, to view log information at the console, or to email log files, use the **pnlog** commands. This command can specify the logging level of the MARS services, as well as the CheckPoint CPMI and LEA logs received by the MARS Appliance. Click on the pnlog command below to display its reference page.

pnlog mailto

pnlog scpto

pnlog setlevel

pnlog show

pnlog mailto

To send an email with the log files appended, use the pnlog mailto command. set the logging level or to view log information at the console, use the **pnlog** command. This command specifies the logging level of the MARS services, as well as the CheckPoint CPMI and LEA logs received by the MARS Appliance.

pnlog mailto {[*smtp_server***] [***sender***] [***recipient***]}**

Syntax Description

smtp_server	
sender	
recipient	

Usage Guidelines

pnlog mailto {[*smtp_server*] [*sender*] [*recipient*]}

The **pnlog mailto** command is an alternative to sending a Feedback e-mail with the log files attached. It sends an e-mail from *sender* to *recipient* using *smtp_server*. The e-mail contains debugging information. These logs contain the logs specified above.

Examples

To send e-mail to bob@exmple.com from admin@example.com using the 192.168.101.5 mail server, enter:

```
pnlog mailto 192.168.101.5 admin@example.com bobc@example.com
```

Related Commands

Command	Description
pnlog scpto	
pnlog setlevel	Sets verbosity level of MARS logs
pnlog show	Displays logfiles

pnlog scpto

pnlog scpto *user*@*server*:*directory*

Syntax Description

user
server
directory

Usage Guidelines

Examples

Related Commands

Command	Description
pnlog mailto	Sends e-mail with log files attached
pnlog setlevel	Sets verbosity level of MARS logs
pnlog show	Displays logfiles

pnlog setlevel

To set the logging level or to view log information at the console, use the **pnlog** command. This command specifies the logging level of the MARS services, as well as the CheckPoint CPMI and LEA logs received by the MARS Appliance.

pnlog setlevel {trace | debug | info | warning | error | critical}

pnlog setlevel cpdebug [*0–9*]

Syntax Description

no keyword	Displays command usage information.
trace	
debug	
info	
warning	
error	
critical	
setlevel debug	
setlevel info	
setlevel warning	
setlevel error	
setlevel critical	
cpdebug [*0–9*]	

Usage Guidelines

The **pnlog setlevel** command specifies how verbose the logs generated by the MARS Appliance services are, with *trace* being the most verbose and *critical* being the least. The default level is *info*. Unless you are actively debugging an issue, Cisco recommends that you use the default value. The *trace* and *debug* options should be used only on the advice of Cisco TAC. Setting a level of *critical* shows only the critical events, while setting a level of *warning* shows all warning or higher events (in other words, it shows warning, error, and critical events). The CLI sets a global output level while the web interface allows you to change this setting for each service (use **pnstatus** to view the list of services). You can access this setting in the web interface by selecting **Admin > System Maintenance > Set Runtime Logging Levels**.

pnlog setlevel cpdebug { **0 | 3 | 9** }

The **pnlog setlevel cpdebug** command sets the output level of the CheckPoint discovery process. You must specify one of three levels: 0, 3, or 9, where 0 disables Check Point debug logging, 3 enables all OPSEC debug logs, and 9 enables all CPMI debug logs. This command is used together with **pnlog show cpdebug** command to study the raw output of CheckPoint Discovery (CPMI) and CheckPoint Log (LEA) sessions. Cisco recommends the use of *9* for debugging and *0* when not actively debugging.

Examples

To set the log level of the MARS Appliance services to debug, enter.

```
pnlog setlevel debug
```

To set the log level of the CheckPoint discovery process to debug, enter:

```
pnlog setlevel cpdebug 9
```

Related Commands

Command	Description
pnlog mailto	Sends e-mail with log files attached
pnlog scpto	
pnlog show	Displays logfiles

pnlog show

To set the logging level or to view log information at the console, use the **pnlog** command. This command specifies the logging level of the MARS services, as well as the CheckPoint CPMI and LEA logs received by the MARS Appliance.

pnlog show {gui | backend | cpdebug}

Syntax Description

no keyword	Displays command usage information.
gui	
backend	
cpdebug	

Usage Guidelines

pnlog show {**gui** | **backend** | **cpdebug**}

The **pnlog show** command provides running output of a particular logfile at the console. You can view one of three logfiles: the GUI logs, the backend logs (shows logs for the processes that the **pnstatus** command reports on), and CheckPoint debug logs. Press Ctrl+C to stop the output of this command.

When using **cpdebug**, you must set the **pnlog setlevel cpdebug** value to 3 or 9, as the default value of 0 turns off all CPE debug messages.

pnlog setlevel cpdebug { **0** | **3** | **9** }

The **pnlog setlevel cpdebug** command sets the output level of the CheckPoint discovery process. You must specify one of three levels: 0, 3, or 9, where 0 disables Check Point debug logging, 3 enables all OPSEC debug logs, and 9 enables all CPMI debug logs. This command is used together with **pnlog show cpdebug** command to study the raw output of CheckPoint Discovery (CPMI) and CheckPoint Log (LEA) sessions. Cisco recommends the use of *9* for debugging and *0* when not actively debugging.

Examples

To set the log level of the CheckPoint discovery process to debug, enter:

```
pnlog setlevel cpdebug 9
```

Related Commands

Command	Description
pnlog mailto	Sends e-mail with log files attached
pnlog scpto	
pnlog setlevel	Sets verbosity level of MARS logs

pnreset

To restore the appliance to the factory default settings (except for the pnadmin account) or to reset a Local Controller to standalone mode, use the **pnreset** command:

pnreset {-h} | {-g} | {-o} | {-j} | {-s}

Syntax Description

no keyword	Default. With no options **pnreset** restores the appliance to factory defaults and purges all configuration and event data (certificate and fingerprints stored to validate reporting devices, topology settings, archived logs, and the license key information).
-h	Displays usage information.
-g	Removes the Global Controller data from a Local Controller, leaving all Local Controller-specific data untouched.
-o	Resets the *tnsnames.ora* file to factory default. The *tnsnames.ora* file is required for the Oracle client to connect to the Oracle server.
-j	Resets the web server scheduler depending on Local Controller's running mode. A restart of web server is enforced.
-s	Resets a Local Controller to standalone mode. It removes the same data as the **-g** option, and in addition, removes the Global Controller connectivity data from the Local Controller and the default Global Controller zone information.

Command History

Release	Modification
4.1.0	This command was introduced with **-g**, **-h**, -**o**, and **-j** options.
4.2.2	The **-s** option was introduced.

Usage Guidelines

The pnreset Command Without Options

The **pnreset** command restores the appliance to factory settings by deleting system configuration and event data stored in the appliance database. This reset process can take between 30 and 60 minutes to complete, depending on the model of the appliance. The **pnreset** command does not reset the password that you have defined for the Administrator (pnadmin) account. To reset the password to factory defaults, you must re-image the appliance using the Recovery DVD.

The **pnreset** command does not re-image the MARS Appliance. You should reimage the appliance when receiving a new appliance not running the most current version of the software or when you need to restore the administrator password to the factory default. For more information on reimaging, refer to Recovery Management, in the Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X.

Before entering the **pnreset** command without an option, disconnect the appliance from the network by unplugging the Ethernet cables from the appliance. Disconnecting from the network ensures that the cursor will return from the command upon completion. You must run **pnreset** without an option using a *direct console* connection, not an ssh console or other network-based connection. This requirement does not apply to **pnreset** when used with one of the options. For more information on console connections, see Establishing a Console Connection in the Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X.

Caution Before executing the **pnreset** command without an option, write down the license key of the appliance. The license key is cleared during the reset process. You must provide this license key during the initial configuration following a reset operation, and it is not restored as part of archived data. This caution does not apply to **pnreset** when used with one of the options.

The -g Option

The **-g** option should be used only when a Global Controller recovery is required. The **-g** option keeps the Global Controller connectivity information on the Local Controller intact, enabling the Local Controller to reconnect as soon as the Global Controller is restored. To purge Global Controller information from the Local Controller, use the ***-s*** option.

The **pnreset -g** command clears the global inspection rules and global user accounts from the Local Controller, which prepares the Local Controller to be managed by the reimaged Global Controller. It does not remove the global user groups; instead they are renamed (appended with a date) and converted to local user groups. You can edit or delete these empty groups after the reset. Because user groups are often used as recipients for rule notifications, they are not deleted to avoid invalidating the Action definition of such rules.

The -o Option

Resets the *tnsnames.ora* file to factory defaults. The *tnsnames.ora* file is required for the Oracle client to connect to Oracle server. If MARS does not pull logs from the Oracle client, this option should never be used. If the *tnsnames.ora* file contains invalid data, MARS may be unable to connect to its internal Oracle database. This option should only be used when errors indicated that MARS has failed to setup an external Oracle server, errors are reported during that setup, and the **pnstatus** command fails to execute due to these connectivity issues.

Caution Do not use the **-o** option to troubleshoot all Oracle client issues. Using this command clears all Oracle client settings from the MARS Appliance, requiring that you re-enter all Oracle client setting using the web interface. Use this option only on direction from the Cisco TAC.

The -j Option

Resets the web server scheduler depending on the Local Controller's running mode. A restart of web server is enforced.

The -s Option

The **-s** option (4.2.2 and more recent) resets a Local Controller to Standalone mode from Monitor mode when the Global Controller cannot completely uncouple from (that is, delete) a Local Controller because of an unreliable network connection. It removes the same data as the **-g** option, removes the Global Controller connectivity data from the Local Controller, and removes the default Global Controller zone information. Use this option in the following cases:

- To reset a Local Controller when a Global Controller that was not running in archive mode crashes. If you plan to restore the Global Controller from an archive, use the **-g** option.
- If the Global Controller is not available or is unable to connect to the Local Controller, preventing you from successfully deleting the Local Controller entry from the Global Controller.
- If a Local Controller delete operation from the Global Controller fails.

Note If the Global Controller is operating properly and there is Global Controller-to-Local Controller connectivity, we recommend deleting the Local Controller entry from the Global Controller.

Examples

To restore the MARS Appliance to the factory defaults, enter:

```
pnreset
```

To prepare for a Global Controller reset or recovery, enter the following command on each Local Controller monitored by the Global Controller:

```
pnreset -g
```

To remove the Global Controller communication information and reset a Local Controller to standalone mode, enter the following command on the target Local Controller:

```
pnreset -s
```

Note You must also delete the Local Controller entry on the Global Controller.

Related Commands

Command	Description
pnstatus	Displays the status of each module running as part of the MARS application.
pnupgrade	Upgrades the software running on the MARS Appliance.

pnrestore

The **pnrestore** command restores data that has been archived using a network attached storage (NAS) device. You can specify the archival settings from the GUI using **Admin > System Maintenance > Data Archiving (see** Configure the Data Archive Setting for the MARS Appliance**)**. For more information on the archive file structure and how the archive works, see Configuring and Performing Appliance Data Backups. For more guidance on restoring, see Guidelines for Restoring.

Note While complete system configuration data is archived, the dynamic data that is archived includes only the data that is received or generated *after* you enable the data archive setting. Therefore, we recommend that you enable archiving before configuring your appliance to receive audit events from reporting devices.

Using the **pnrestore** command, you can restore three types of data:

- **MARS OS—**Restores the operating system (OS), including any upgrades that applied before the most recent archive was performed.

Note The version of MARS software running on the appliance to be restored must match the version recorded in the archive. For example, if the data archive is for version 4.1.4, you must re-image the MARS Appliance to version 4.1.4, not older or newer, before using the **pnrestore** command to recover the system configuration and events.

- **System configuration data—**Restores system configuration data, such as network settings, reporting devices, custom inspection rules, event types, reports, administrative accounts, archival settings, cases, and any other data that you have entered. It also, as of 4.2.1, includes the specific incident and event data associated with cases. It does not restore all dynamic data, just that data associated with cases.
- **Dynamic data—**Restores real event data that came from reporting devices, including incidents generated from events.

  Note Prior to 4.2.1, performing a restore of just the configuration data resulted in incomplete data required to reconstruct existing cases: all open cases reference incidents and sessions. If this dynamic data is not restored, the cases could reference invalid incident and session IDs. To restore cases for releases prior to 4.2.1, you perform a full restore (mode 2).

To restore archived appliance data, use the **pnrestore** command:

pnrestore -m 1 -p *NFSSeverIP***:/***archive_path* **-t** *start_time*

—or—

pnrestore -m 2 -p *NFSSeverIP***:/***archive_path* **-t** *start_time*

—or—

pnrestore -m 3 -r 1 -p *NFSSeverIP***:/***archive_path* **-t** *start_time* **[-e** *end_time* **-s** *NFSSeverIP***:/***stagingAreaPath***]**

—or—

```
pnrestore -m 4-r 1 -p NFSSeverIP:/archive_path -t start_time [-e end_time -s
    NFSSeverIP:/stagingAreaPath]
```

—or—

```
pnrestore -m 5
```

Command History

Release	Modification
4.1.1	Mode 5 appears (*-m 5* option).
5.2.4	End time (*-e*), stage path area (*-s*), and *-r 1* options appear.

Syntax Description

No keyword or option	Displays the command's usage guidelines.
-m	Restoring mode. Three modes are available: 1 (default), 2, or 5. The mode determines what type of data is restored and from where the data is restored. Table 1-2 identifies what data is restored for each option. **Note** Mode 5 restores from a backup in the local database; you cannot use it to restore from a NFS archive. As such, you not need to have archiving enabled to perform this restore operation. The configuration data is backed up every night on the appliance. Beware that if you upgrade to a newer release and attempt a restore before that configuration has been backed up, the restore will fail.
-h	Displays the detailed command's usage guidelines.
-t	Restores the data dated from this time through the most current archive date. Use *mm/dd/yy:hh* format. This option is required when you select mode r 2.
-e	(5.2.4 and later) Used in conjunction with -t and -s, this parameter allows you to specify the end time (endTime) of the data restore range. Used to restore a past range of data.
-s	(5.2.4 and later) Used in conjunction with -t and -s, this parameter allows you to specify the path (stagePath) on the NFS server to which to copy the range of data. This option is used to create a staging area from which you can restore a past range of data.

-p	Name of the directory where the archived data is stored. You must identify the NFS server by IP address, separated by a :/ and then the pathname `NFSSeverIP:/archive_path`. Where *NFSSeverIP* is the value specified in the Remote Host IP field and *archive_path* is the value specified in the Remote Path field in the settings found in the web interface at **Admin > System Maintenance > Data Archiving**. For more information on these settings, see Configure the Data Archive Setting for the MARS Appliance.
-r 1	(5.2.4 and later) Used in conjunction with modes 3 and 4 only. Skips restoring the OS binary; instead only the configuration and dynamic data is restored. Because the version used to write out the archive for a particular time slice may predate the version most recently stored on the NFS server, these modes prevent MARS from overwriting the OS installed in the appliance to read the specified time slice's data.

Table 1-2 pnrestore Mode Description

Restore Mode	Restore OS?	Restore System Configuration?	Restore Dynamic Data?
1 (default)	Yes	Yes	Partial[1]
2	Yes	Yes	Yes
3 -r 1	No	Yes	No
4 -r 1	No	Yes	Yes
5	No	Yes[2]	No

[1] The incident and event data associated with cases is restored; however, other dynamic data is not.

[2] Mode 5 restores data from a local configuration file on the MARS Appliance, not an NFS server.

Examples

You can use the restore feature to complete different restoring tasks, such as:

- Perform a partial restore on the same MARS Appliance using the local backup of the configuration data; it essentially restores the previous days' configuration backup. Use the **pnrestore** command, mode 5. For example, in the CLI menu of the appliance, enter:

```
pnrestore -m 5
```

- Perform a partial restore on the same MARS Appliance using the archived data (including the OS and all data), but restoring only the event data generated since January 2, 2006 through the current date. Use the **pnrestore** command, mode 2. For example, in the CLI menu of the appliance, enter:

```
pnrestore -m 2 -p 192.168.1.1:/archive/CS_MARS1 -t 01/02/06:0
```

- Archive and restore data to the same MARS Appliance or a different MARS Appliance of the same model. From the appliance where you want to archive the data, use the GUI to configure archiving. From the appliance to which you want to copy the archived data, use the **pnrestore** command.

  For example, if you only want to copy the OS and the system configuration data, you should use mode 1 of the restore command. For example in the CLI menu of the new appliance, enter:

```
pnrestore -m 1 -p NFSSeverIPOfOldBox:/archive/CS_MARS1
```

Caution When restoring Local Controller data, problems can arise if you attempt to restore dynamic data from a bigger appliance to a smaller appliance. In such cases, use mode 1.

- Create a staging area that contains a range of data and determine the correct version of MARS to use when restoring the selected data. Depending on the generation of hardware that generated the archive, pnrestore copies the data range to a target directory. Upon completion, pnrestore displays the version of MARS to use to stage the ranged restore as well as the correct restore parameter and NFS directory to use.

  Note Upon completion of a staged restore, use the web interface to change the hostname, IP address, and license settings of the MARS Appliance to the appropriate values.

  For example, if you want to stage data between 10/01/06 and 11/01/06 to the corresponding directory under the *stageAreaPath* directory, enter:

  ```
  pnrestore -t 10/01/06:00 -e 11/01/06:00 -p nfsIp:/archive -s nfsIp:/stageAreaPath
  ```

- Restore only the configuration and runtime data from October 1, 2006 at midnight to November 1 2006 at midnight, with the archive at 10.1.1.1 and the corresponding directory under the *stageAreaPath* directory at 10.1.10.15.

  ```
  pnrestore –m 4 –r 1 -t 10/01/06:00 -e 11/01/06:00 -p 10.1.1.1:/archive -s 
  10.1.10.15:/stagingArea
  ```

pnsshfs

To handle outdated SSH keys, use the **pnsshfs** command.

pnstart [<*username*>@]<*host IP*>*:*<*dir*> *[-v]*

Syntax Description

<*username*>@	[Optional] The login username to the SSHFS archive server
<*host IP*>*:*	The IP address of SSHFS archive server
<*dir*>	The archive path
-v	[Optional] Verbose command output

Usage Guidelines

Before this command, archiving with supported SFTP/SSHFS servers was a problem because if the archive server was re-imaged, the stored SSH key on CS-MARS could not be removed. The pnsshfs command is implemented to handle outdated SSH keys. The SSH behavior used by pnsshfs corresponds to the setting in Admin > System Parameters > SSL/SSH Settings (always accept, accept first time and prompt with changed, or always prompt).

Command History

Release	Modification
6.1.1	This command was introduced for the CS-MARS.

Examples

The following pnsshfs command stores a new key

```
[pnadmin]$ pnsshfs root@10.2.3.10:/archive/ymchou/LC227
The fingerprint for RSA key sent by the remote is
f3:71:9c:0d:fa:f5:dc:5d:79:86:fb:a8:ad:66:ae:33
Do you want to use this key? (yes/no) yes
Type password:
pnsshfs: check success
```

pnstart

To manually start the MARS application running on the appliance from the serial console, use the **pnstart** command.

pnstart

Syntax Description

This command has no arguments or keywords.

Examples

The following command starts the MARS application running on the appliance:

```
pnstart
```

pnstatus

To show the status of each module running as part of the MARS application from the serial console, use the **pnstatus** command.

pnstatus

Note For a description of the processes and services, see List of Backend Services and Processes.

All services should be running on a Local Controller. However, a Global Controller only has four services running: autoupdate, graphgen, pnarchiver, and superV—all other services are stopped.

Syntax Description

This command has no arguments or keywords.

Examples

The following example displays the status of each module running on the MARS Appliance:

```
[pnadmin]$ version
6.0.1 (2955) 30
[pnadmin]$ pnstatus
Module                          State           Uptime
DbIncidentLoaderSrv             RUNNING         90-16:14:33
KeywordQuerySrv                 RUNNING         90-16:14:35
autoupdate                      RUNNING         90-16:14:34
csdam                           RUNNING         90-16:14:35
csiosips                        RUNNING         90-16:14:33
csips                           RUNNING         90-16:14:35
cswin                           RUNNING         90-16:14:33
device_monitor                  RUNNING         90-16:14:34
discover                        RUNNING         85-21:08:50
graphgen                        RUNNING         05:15:45
pnarchiver                      RUNNING         90-16:14:36
pndbpurger                      RUNNING         90-16:14:35
pnesloader                      RUNNING         90-16:14:36
pnmac                           RUNNING         90-16:14:36
pnparser                        RUNNING         74-13:09:55
process_event_srv               RUNNING         49-17:54:26
process_inlinerep_srv           RUNNING         90-16:14:35
process_postfire_srv            RUNNING         90-16:14:36
process_query_srv               RUNNING         90-16:14:36
securesyslog                    RUNNING         90-16:14:36
superV                          RUNNING         90-16:14:36
```

pnstop

To stop the MARS application running on the appliance from the serial console, use the **pnstop** command.

pnstop

Syntax Description

This command has no arguments or keywords.

Examples

The following command stops the MARS application running on the appliance:

```
pnstop
```

pnupgrade

To upgrade the software image running on the MARS Appliance, use the **pnupgrade** command. The **pnupgrade** command is not easily decipherable when presented in standard Cisco IOS command syntax; For this command page, it is parsed into more decipherable components.

pnupgrade [options] {url}

Keyword	Expanded Syntax
options	**[-d] [-h][-l] [-n] [-p] [-r] [-s]** **[-u** *login***:***passwd***]** **[-U** *proxylogin***:***proxypasswd***]** **[-x** *proxyservr:proxyport***]**

url	{{**ftp** | **https** | **http**}
	://*url-path***/csmars-***version***.zip**} |
	{**cdrom://***cdpath* **/ csmars-***version***.zip**}

url-path	*host-port / path*
host-port	[*login* [:*passwd*]@] *host* [:*port*]

Syntax Description

-d	Displays a confirmation to continue prompt if the upgrade package hey reboot
-h	Displays the help text message
-l	Displays the upgrade log
-n	Disables operation timeout
-p	Preempts the previous upgrade manager
-r	Forces a system reboot after the upgrade completes
-s	Continues upgrade even if sanity check fails
-u *login***:***passwd*	Sets upgrade server login and password
-U *proxylogin***:***proxypasswd*	Sets proxy server login and password
-x *proxyname:proxyport*	Indicates HTTP proxy server on specified port
ftp	Specifies File Transfer Protocol as transport method
https	Specifies Hyper Text Transfer Protocol over SSL as transport method
http	Specifies Hyper Text Transfer Protocol as transport method
url-path	See Expanded Syntax description in previous table.
cdrom	Specifies that the upgrade package is located on the MARS DVD drive
cdpath	Path to the upgrade package on a CD-ROM or DVD
csmars-*version***.zip**	Upgrade package name. For example, csmars-6.0.1-2428.zip
host-port	See Expanded Syntax description in previous table.
path	Path to the upgrade package on the upgrade server
login	Login name for upgrade server
passwd	Password for upgrade server

host	Hostname of upgrade server
port	Port of upgrade server

Usage Guidelines

The **pnupgrade** command is executed from an SSH or a console connection. If the SSH session terminates during the upgrade, the upgrade continues uninterrupted.

The **pnupgrade** command can load an image file stored on the following media:

- Internal Upgrade Server (accessed directly or through a proxy server)
- CD-ROM or DVD

See the Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X, Checklist for Upgrading the Appliance Software, for details on obtaining upgrade images and preparing the Internal Upgrade Server.

The procedure to upgrade MARS from the CLI is at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/initial/configuration/admin.html#wp1107979

The supported transport protocols are FTP, HTTPS, and HTTP. The CD-ROM and DVD methods access the MARS DVD drive.

For the FTP, HTTPS, and HTTP methods, you can configure a specific port number instead of relying on the default port number for that service.

You can also specify a login and password as part of the URL syntax instead of using the **-u** option.

Note When using the HTTPS syntax, if the certificate of the upgrade server changes between upgrades, you are prompted by pnupgrade to accept the new certificate before the upgrade continues.

Table 1-3 discusses usage guidelines for some of the **pnupgrade** options.

Table 1-3 Usage Note—pnupgrade Command Options

Command Option	Usage Notes
-d (desist)	If the upgrade package being applied requires a system reboot, the -d option displays a confirmation-to-continue prompt before proceeding with the upgrade. This allows you to cancel the upgrade before it begins.
-n (no timeout)	Overrides the timeout of the upgrade script. In some instances, the time to complete an upgrade task can exceed the system allocated timeout, causing the upgrade to terminate (For example, some data upgrade packages require extensive database integrity checks). The -n option allows the upgrade to run to completion. **Caution** Cisco cautions against using the -n option on the first upgrade attempt.
-p (preempt)	The -p option terminates any in-progress upgrade then runs the upgrade with the package specified in the command line. An upgrade can be in-progress but not apparent from an SSH session. For example, if the SSH session that initiated an upgrade is terminated during the upgrade, some CLI-related upgrade processes are closed but backend upgrade processes continue to run. If another pnupgrade command is issued through a new SSH session, thats upgrade will be rejected unless the -p option is used to terminate the upgrade still running. The newest upgrade begins immediately after the still running upgrade is terminated.
-r (reboot)	Forces the CS-MARS to reboot after the upgrade has completed.
-s (sanity check)	A sanity check determines if necessary resource conditions are met for the specified upgrade package, for example sufficient temporary disk space. You can ignore negative results and the upgrade will continue. Results of the sanity check are displayed to the screen and recorded in the /tmp/debug_loader file for use by Cisco TAC. **Note** Failed sanity checks do not cause MARS to abort the upgrade.

Table 1-3 Usage Note—pnupgrade Command Options

Command Option	Usage Notes

-u (server login and password)	The upgrade server login and password can also be included as part of the URL. For example, the following commands are equivalent:
	`pnupgrade -u mylogin:mypasswd https://10.2.3.4/upgrade/packages/ csmars-6.0.1.3016.zip`
	`pnupgrade https://mylogin:mypasswd @10.2.3.4/upgrade/packages/ csmars-6.0.1.3016.zip`

-U (proxy server login and password)	The login and password required by the proxy server. Use -U together with the -x option.
-x (proxy server address and port number)	The IP address and port number of the proxy server. Use the -U option if a login and password are required.

Upgrade Log File

The **pnupgrade -l** command displays a log of each step that was performed during the most recent upgrade. This log file can identify which steps failed or hung in a failed upgrade attempt.

Image Management Troubleshooting

If the upgrade is done with the GUI, any errors encountered are prominently displayed in the Upgrade Status Logs section.

For CLI upgrade errors, check the **pnupgrade -l** log file first. Cisco TAC can check for the existence of any other failed upgrade log files with the expert password.

For Global Controller and Local Controller image management problems, make sure that the status for each Local Controller status is "Active." If it is not "Active," then go to Admin -> LC Management for more troubleshooting information.

Examples

The following example displays the upgrade log file:

```
[pnadmin]$pnupgrade -l
```

The following example specifies username "aladdin" and password "opensesame" to authenticate to the HTTPS Internal Upgrade Server "10.1.1.2" using default port numbers. The upgrade package is retrieved from the "/packages" directory:

```
[pnadmin]$pnupgrade -u aladdin:opensesame https://10.1.1.2/packages/csmars-6.0.1.2747.zip
```

The following example specifies no timeout during the upgrade and port 8080 of the HTTP Internal Upgrade Server, with no authentication:

```
[pnadmin]$pnupgrade -n http://pnadmin@10.1.1.1:8080/csmars-6.0.1.4168.zip
```

The following example specifies the username "ybother" without a password to authenticate to the HTTPS Internal Upgrade Server using default port numbers. The upgrade package is retrieved from the "/packages" directory:

```
[pnadmin]$pnupgrade -u ybother https://10.2.3.8/packages/csmars-6.0.1-2424.zip
```

The following example specifies the proxy server “myproxy” to retrieve the upgrade file from the default directory of the Internal Upgrade Server “10.1.1.1” using HTTP on default ports (both proxy and Internal Upgrade Server). The username “myname” and password “mypass” authenticate to the proxy server; The login “me” with no password authenticates to the Internal Upgrade Server:

```
[pnadmin]$pnupgrade -x myproxy -U myname:mypass http://me@10.1.1.1/csmars-6.0.1-2428.zip
```

The following example performs an upgrade from the MARS DVD drive:

```
[pnadmin]$pnupgrade cdrom://csmars-6.0.1-2168.zip
```

The following example demonstrates the -d option with an upgrade package that requires a MARS reboot:

```
[pnadmin]$pnupgrade -d
https://mylogin:mypasswd@10.1.2.1/upgrade/packages/csmars-6.0.1.3016.zip
CSMARS Upgrade...........[7370]
Loading..................[csmars-6.0.1.3016.zip]
    User.................[mylogin]
    Protocol.............[https]
    Host.................[10.1.2.1]
    Path.................[upgrade/packages/csmars-6.0.1.3016.zip]
    Modified.............[Wed, 30 Jul 2008 05:05:49 GMT]
    Size.................[318541040]
######################################################################### 100.0%
Upgrade..................[pnmars]
    From.................[6.0.1.3000.30]
    To...................[6.0.1.3016.30]
Strip Meta Data..........[csmars-6.0.1.3016.zip]
[Alert][confirm_upgrade/98]: reboot after upgrade is completed.
/dev/hda1 has gone 28 times of booting without being checked, will be checked at the
coming reboot.
An estimated 1 minute increase of booting time will occur at the coming reboot.
fsck will be required on 1 partition at next reboot.
Continue upgrade? yes/[no]
```

Related Commands

Command	Description
pnlog mailto	Sends a Feedback e-mail with the log files attached.
predictfsck	Predicts the duration of the file system check that will occur if the Cisco Security MARS is rebooted.

predictfsck

To predict the duration of the file system check that will occur if the Cisco Security MARS is rebooted, enter the **predictfsck** command.

predictfsck

Syntax Description

There are no keywords or arguments for this command.

Usage Guidelines

If a user installs an upgrade package that requires a reboot, a file system check (FSCK) is run after the reboot. The **predictfsck** command predicts the duration of the required FSCK.

Examples

The following examples display **predictfsck** output for a Cisco Security MARS that requires a file system check upon reboot.

```
[pnadmin]$ predictfsck
/dev/hda1 has gone 74 times of booting without being checked, will be checked at the
coming reboot.
An estimated 1 minute increase of booting time will occur at the coming reboot.
fsck will be required on 1 partition at next reboot.
```

The following examples display **predictfsck** output for a Cisco Security MARS that does not require a file system check upon reboot.

```
[pnadmin]$ predictfsck
fsck will not be required at next reboot.
[pnadmin]$
```

Related Commands

Command	Description
pnupgrade	Upgrades the software image running on the MARS Appliance.
pnrestore	Restores data that has been archived using a network attached storage (NAS) device.
reboot	Reboots the MARS Appliance.
shutdown	Shuts down and powers-off the MARS appliance.

raidstatus

To view the status of the RAID array and of the individual hard drives, use the **raidstatus** command.

raidstatus

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
4.2.1	This command introduced for Generation 1 hardware
5.2.4	This command was introduced for Generation 2 hardware
5.3.2	Support for the MARS 55 was added.

Usage Guidelines

The **raidstatus** command is used with the **hotswap** command to replace component hard drives of the MARS Appliance Raid array.

For information on RAID hotswapping procedures and hard drive alerts, see the chapter, "*Hardware Maintenance Task*" in the *Cisco Security MARS Hardware Installation and Maintenance Guide 6.X* at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/hardware/installation/guide/hig_mars_6x.html

Examples

Raidstatus Examples for 55, 110R, 110, 210, GC2R and GC2

The following example displays a MARS 55 with a failed hard drive:

```
[pnadmin]$ raidstatus
RAID Controller Information:
-------------------------------------------------------
Product Name    : Intel Embedded Server RAID Technology
Driver Version  : 05.08y
Controller Type : SATA

Adapter  Raid Type  Status         Stripe    Size
------------------------------------------------------
 a0      Raid 1     Degraded       64 KB     476772 MB

Port Status       Size        Model            Serial #        Write Cache
--------------------------------------------------------------------------
0    Online       476772 MB   HDS725050KLA360  KRVN0AZBH5R3LJ  Enabled
1    Failed       476772 MB   HDS725050KLA360  KRVN0AZBH5R8RJ  Enabled
```

In the following example, the MARS 210 RAID array is fully operational and redundant, that is, adapter a0 Raid-10 status is optimal, and all of the hard drives are online.

```
[pnadmin]$ raidstatus
Adapter Information:
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version :  1.03.00-0211
BIOS Version     : MT30
```

```
Adapter RaidType        Status  Stripe  Size          Cache
---------------------------------------------------------------
a0      Raid-10         Optimal 64kB    2097151MB     Enabled

PD     Status  Size & Block                           Model                    Serial#
-----------------------------------------------------------------------------------------
p0     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          CQD017CET
p1     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02EMY
p2     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02ELS
p3     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02D0A
p4     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD01T1P
p5     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02BZ7
```

In the following example, the MARS 210 RAID array is shown degraded because hard drive 3 (p3) has failed. The RAID array is functional, but not fully redundant because the p2+p3 RAID 1 pair is compromised.

```
[pnadmin]$ raidstatus
Adapter Information: -------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version : 1.03.00-0211
BIOS Version     : MT30
Adapter RaidType        Status          Stripe  Size            Cache
-------------------------------------------------------------------------------
a0      Raid-10         Optimal         64kB    2097151MB       Enabled

PD     Status  Size & Block                           Model                    Serial#
-----------------------------------------------------------------------------------------
p0     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          CQD017CET
p1     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02EMY
p2     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02ELS
p3     Failed  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02D0A
p4     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD01T1P
p5     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02BZ7
```

In the following example, hard drive 3 has been replaced with the **hotswap** command, and is being rebuilt into the the MARS 210 Raid Array. The Array remains degraded until p3 has Online status. The progress message at the bottom shows percentage complete and time elapsed in the rebuild process.

```
[pnadmin]$ raidstatus
Adapter Information: C3QD02C0K
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version :  1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size          Cache
---------------------------------------------------------------
a0      Raid-10         Degraded 64kB    2097151MB     Enabled

PD     Status  Size & Block                           Model                    Serial#
-----------------------------------------------------------------------------------------
p0     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          CQD017CET
p1     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02EMY
p2     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02ELS
p3     Rebuild 715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02C0K
p4     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD01T1P
p5     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02BZ7

Rebuild Progress on Device at Enclosure 20, Slot 2 Completed 71% in 279 Minutes.
```

Raidstatus Examples for MARS 50, 100, 100e, 200, GC and GCm

Example 1-1 displays the output of the raidstatus command executed on a Local Controller 200. Table 1-4 describes the output fields.

Example 1-1 Example of raidstatus CLI Command Output for a Local Controller 200

```
[PNADMIN]$ raidstatus

CONTROLLER: C0
-------------
DRIVER:    1.02.00.037
MODEL:     7506-8
FW:        FE7X 1.05.00.068
BIOS:      BE7X 1.08.00.048
MONITOR:   ME7X 1.01.00.040
SERIAL #:  L14104A5090383
PCB:       REV4
PCHIP:     1.30-66
ACHIP:     3.20


# OF UNITS: 1
UNIT 0: RAID 10 931.54 GB ( 1953580032 BLOCKS): REBUILDING (75%)

# OF PORTS: 8
PORT 0: WDC WD2500JB-19GVA0 WD-WCAL73129135 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 1: WDC WD2500JB-19GVA0 WD-WCAL73291174 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 2: WDC WD2500JB-19GVA0 WD-WCAL73157538 232.88 GB (488397168 BLOCKS)
: OK(NO UNIT)
PORT 3: WDC WD2500JB-98GVA0 WD-WMAL72243570 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 4: WDC WD2500JB-00GVA0 WD-WCAL73883655 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 5: WDC WD2500JB-19GVA0 WD-WCAL73290905 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 6: WDC WD2500JB-98GVA0 WD-WCAL73693347 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 7: WDC WD2500JB-98GVA0 WD-WMAL72244432 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
UNIT /C0/U0
---------------------
STATUS:         REBUILDING
UNIT TYPE:      RAID 10
STRIPE SIZE:    64K
SIZE:           931.54 GB (1953580032 BLOCKS)
# OF SUBUNITS: 4

SUBUNIT 0:     RAID 1: OK

SUBUNIT 0:     CBOD: OK
PHYSICAL PORT: 7
LOGICAL  PORT: 0

SUBUNIT 1:     CBOD: OK
PHYSICAL PORT: 4
LOGICAL  PORT: 1
```

```
SUBUNIT 1:    RAID 1: REBUILDING (1%)

SUBUNIT 0:    CBOD: DEGRADED
PHYSICAL PORT: 6
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 3
LOGICAL  PORT: 1

SUBUNIT 2:    RAID 1: DEGRADED

SUBUNIT 0:    CBOD: OK
PHYSICAL PORT: 5
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 0
LOGICAL  PORT: 1
SUBUNIT 3:    RAID 1: OK

SUBUNIT 0:    CBOD: OK
PHYSICAL PORT: 1
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 0
LOGICAL  PORT: 1
```

Table 1-4 Explanation of Output Fields for raidstatus CLI Command for MARS 50, 100E, 100, 200, GCM, and GC

Output Field	Description
`FW:       FE7X 1.05.00.068`	Indicates version of controller card firmware.
`STATUS:        REBUILDING`	Current status of entire array. • **OK**—The array and subunits are in good order and operating at optimal efficiency. • **Rebuilding**—A subunit is being rebuilt. Array efficiency is not yet optimal. • **Degraded**—At least one physical disk in the array cannot be accessed.

Table 1-4 Explanation of Output Fields for raidstatus CLI Command for MARS 50, 100E, 100, 200, GCM, and GC (continued)

Output Field	Description
`# OF UNITS: 1 UNIT 0: RAID 10 931.54 GB ( 1953580032 BLOCKS): REBUILDING (75%)`	**Units**—Indicates the number of virtual drives the entire RAID configuration represents. In this case, the array acts as one virtual hard drive or unit. **Unit**—Identifies the RAID level, array size, and array status statistics of the specified unit. The total array size does not include the RAID overhead bytes. The status may be as follows: • **OK**—The array and subunits are in good order and operating at optimal efficiency. • **Rebuilding**—A subunit is being rebuilt. Array efficiency is not yet optimal. • **Degraded**—At least one physical disk in the array cannot be accessed. Troubleshooting is advised to prevent possible data loss.
`# OF PORTS: 8`	Indicates the number of hard drives in the array.

Table 1-4 Explanation of Output Fields for raidstatus CLI Command for MARS 50, 100E, 100, 200, GCM, and GC (continued)

Output Field	Description

`PORT 0: WDC WD2500JB-19GVA0 WD-WCAL73129135`
`232.88 GB (488397168 BLOCKS)`
`: OK(UNIT 0)`
	Indicates the model, serial number, size, and operational status of a hard drive related to the port. If a hard drive is not present or cannot be accessed, this output does not appear for that port.

`SUBUNIT 1:    RAID 1: REBUILDING (1%)`
 	
`SUBUNIT 0:    CBOD: DEGRADED`
`PHYSICAL PORT: 6`
`LOGICAL  PORT: 0`
 	
`SUBUNIT 1:    CBOD: OK`
`PHYSICAL PORT: 3`
`LOGICAL  PORT: 1`
	A MARS RAID 10 configuration comprises multiple RAID 1 subunits, each RAID 1 subunit configured with two drives. The MARS 100 and 100e appliances have subunits numbered 0,1, and 2. MARS 200 appliances and Global Controllers have subunits 0,1,2, and 3.
	The two drives in each RAID 1 subunits have unique physical port numbers.
	The RAID 1 subunit status values are as follows:
	• **OK**—The subunit is in good order and operating at optimal efficiency.
	• **Rebuilding**—The subunit is being rebuilt, efficiency is not yet optimal.
	• **Degraded**—At least one physical disk in the array cannot be accessed.
	The rebuild processes can take between 90 minutes and two hours to complete, depending on the amount of data on the disk. Subunits are rebuilt one subunit at a time. The percentage complete indicator tells you which subunit is currently being rebuilt.
	The **Physical Port** number appears as N/A when the associated drive bay is empty.
	Individual drive status is shown in the **CBOD:** field. CDBOD status can be OK or DEGRADED.

Related Commands

Command	Description
hotswap	Specifies that a designated hard drive is to be removed or added to a RAID array.
show inventory	Displays information on chassis, hard drives and power supplies

reboot

To reboot the MARS Appliance from the serial console, use the **reboot** command.

reboot

Caution The reboot is immediate and you are not prompted to confirm.

Syntax Description

This command has no arguments or keywords.

Examples

The following command reboots the appliance:

```
reboot
```

Related Commands

Command	Description
predictfsck	Predicts the duration of the file system check that will occur if the Cisco Security MARS is rebooted.

route

The **route** command manipulates the MARS Appliance's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the **ifconfig** command.

When the add or del options are used, the **route** command modifies the routing tables. Without these options, the **route** command displays the current contents of the routing tables.

To list the kernel routing tables, enter:

route [**-nNve**] [**-FC**]

To add a route to the routing table, enter:

route [**-v**] [**-FC**] **add** [**-net** | **-host**] *target* [*netmask*] [*gateway*] [**metric** *N*] [**mss** *M*] [**window** *W*] [**irtt** *I*] [**reject**] [**mod**] [**dyn**] [**reinstate**] [[**dev**] *inf_local*]

To delete a route from the routing table, enter:

route [**-v**] [**-FC**] **del** [**-net** | **-host**] *target* [*netmask*] [*gateway*] [**metric** *N*] [[**dev**] *inf_local*]

To display detailed usage syntax for the command, enter:

route -h

To display version/author information and exit, enter:

route -V

Syntax Description

no keyword or option	Displays current configuration of the MARS interfaces.
add	Add a route to the table.
-C	Display routing cache instead of FIB
del	Delete the specified route from the table.
-e	Display extended information.
-F	Display Forwarding Information Base (FIB), which is the default.
gateway	IP address of the gateway for this route.
-*h*	Displays the detailed command's usage guidelines.
-host	Identifies the route a host route.
irtt	I Set the initial round trip time (irtt) for TCP connections over this route to *I* milliseconds (1-12000). If omitted, the default value is 300ms.
mms *M*	Set the TCP Maximum Segment Size (MSS) for connections over this route to M bytes. The default is the device MTU minus headers, or a lower MTU when path mtu discovery occurred.
mod, dyn	Reinstate install a dynamic or modified route. These flags are for diagnostic purposes, and are generally only set by routing daemons.
-n	Display numeric values for addresses; don't resolve hostnames.
-net	Identifies the route as a network route.
netmask	Network mask that corresponds to the *ip_addr* value.

reject	Install a blocking route, which forces a route lookup to fail. Use this feature, for example, to mask out networks before using the default route. Do not use for firewalling.
target	IP address of the host or network for which you are defining a route.
-v	Display verbose information.
window W	Set the TCP window size for connections over this route to *W* bytes.

Usage Guidelines

The **route** command is a standard Linux command.

script

Use the restricted script command mode to execute provided script:

script [-b] *program*

Syntax Description

-b	
program	Identifies the name of the script to run.

Command History

Release	**Modification**
4.3.1	This command was introduced in the 4.3.1 release.
5.3.1	This command was introduced in the 5.3.1 release.

Usage Guidelines

The following scripts are available from the restricted script command mode:

- **get_mars_summary_info.sh**— Gather high level statistics about the configuration and topology for the MARS Appliance.

Examples

The following example gathers high level statistics about the MARS Appliance’s configuration and topology.

```
[pnadmin]$ script get_mars_summary_info.sh
Collecting MARS summary info from the DB in HTML format
Started at Fri Sep 14 05:50:10 PDT 2007
Use 'pnlog mailto' command to include it in the logs
This may take several minutes to complete. Use Ctrl+C in case you need to interrupt.
Completed at Fri Sep 14 05:50:10 PDT 2007
[pnadmin]$
```

show healthinfo

To display the operational status of key components in the appliance use the **show healthinfo** command.

show healthinfo

Syntax Description

There are no arguments or keywords for this command.

Command History

Release	Modification
5.2.4	This command was introduced for the MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC.
6.0.1	This command was introduced for the MARS 20, 50, 100E, 100, 200, GCM, and GC.

Usage Guidelines

The **show healthinfo** command displays the operational status of critical components, such as fans, CPUs, hard drives, Ethernet interfaces, power supplies, backup battery units, memory usage, and the operating system.

Power Supply

In the command output for Power Supply, PS1 is the lower power supply, PS2 is the upper power supply. In normal operation, PS1 supplies most of the power requirements, and PS2 is the redundant power supply.

Ethernet Card Status

In the command output for Ethernet, eth0 is integrated NIC 1, eth1 is integrated NIC 2; eth2 and eth3 are not supported.

Raid Battery Backup Unit

In the command output for BBU, the relative state of charge is directly proportional to the battery backup time ($100\%_{\text{charge}} = 72_{\text{hours}}$).

For more information on RAID BBU and power supply procedures, see the chapter, "Hardware Maintenance Tasks—MARS 55, 110R, 110, 210, GC2R, and GC2" in the *Cisco Security MARS Hardware Installation and Maintenance Guide, 6.X* at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/hardware/installation/guide/maintain_gen2.html

Examples

The following example dispays the health monitoring information on a MARS 110.

```
[pnadmin]$ show healthinfo
CPU Information:
Processor       Vendor ID       Model   CPU(MHZ)
 0 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
 1 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
 2 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
 3 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
```

```
Memory Information:
MemTotal: 4137832 kB    MemFree: 18812 kB

Fan ID  RPM             Status
----------------------------------
Fan 1   7052 RPM        ok
Fan 2   7611 RPM        ok
Fan 3   7095 RPM        ok
Fan 4   7568 RPM        ok
Fan 5   10416 RPM       ok
Fan 6   9610 RPM        ok

CPU     Temperature     Status
--------------------------------
CPU1 VRD Temp   0x00    ok
CPU2 VRD Temp   0x00    ok
CPU1 Vcc OOR    0x00    ok
CPU2 Vcc OOR    0x00    ok

Power Supply            Value   Status
----------------------------------------
PS1 AC Current  2.36 Amps       ok
PS2 AC Current  0.12 Amps       ok
PS1 +12V Current        21 Amps ok
PS2 +12V Current        0 Amps  ok
PS1 +12V Power  248 Watts       ok
PS2 +12V Power  0 Watts ok
PS1 Status     0x01     ok
PS2 Status     0x09     ok

Ethernet card status
eth0 is up
eth1 is up
eth2 is down
eth3 is down

Flash driver is Online

BBU information :
Relative state of charge : 93 %
Full charge capacity : 920 mAh
Remain capacity : 858 mAh

OS information :
Linux SJ-LC-17 2.6.9-42.0.2.ELsmp #1 SMP Thu Aug 17 18:00:32 EDT 2006 i686 i686 i386
GNU/Linux
```

The following example dispays the health monitoring information on a MARS 20.

Related Commands

Command	Description
ifconfig	Displays or modifies the IP address and network mask of the network interfaces.
show inventory	Displays identifying details of essential components in the appliance.

show inventory

To display an inventory and serial numbers, of essential components in the MARS Appliance, use the **show inventory** command.

show inventory

Syntax Description

There are no arguments or keywords for this command.

Command History

Release	Modification
5.2.4	This command was introduced for the MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC.
6.0.1	This command was introduced for the MARS 20, 50, 100E, 100, 200, GCM, and GC.

Usage Guidelines

The **show inventory** command displays the part identification string (PID) and serial numbers of the chassis, hard drives, RAID battery backup unit, and power supplies.

Examples

The following example displays the inventory of a MARS 110 Local Controller:

```
[pnadmin]$ show inventory
NAME: "Chassis",  DESCR: "CS-MARS-110 Local Controller"
PID: CS-MARS-110,       VID: V01,       SN: M1100000027

RAID Information:
NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GFH

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG00KH4

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GCH

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GE4

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GHJ

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GGV

RAID Battery Backup Unit Information:
NAME: "Battery", DESCR: "MARS110/210/GC2 RAID Controller Back-Up Battery"
PID: CS-MARS-X10-BB,     VID:   ,       SN: 313

Power Supply Information:
NAME: "Power supply",  DESCR: "MARS110/210/GC2 Power Supply Module"
PID: CS-MARS-D750-PS,    VID:   ,        SN:  DLD0636022220

NAME: "Power supply",  DESCR: "MARS110/210/GC2 Power Supply Module"
```

```
PID: CS-MARS-D750-PS,    VID:   ,        SN:  DLD0621008449
```

The following example displays the inventory of a MARS 20:

```
[pnadmin]$ show inventory
NAME: "Chassis",  DESCR: "CS-MARS-20 Local Controller"
PID: CS-MARS-20,        VID: ,  SN: 003048832C34
```

Related Commands

Command	Description
show healthinfo	Displays operational status of appliance components.

shutdown

To shut down and power-off the MARS appliance from the serial console, use the **shutdown** command.

shutdown

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

To turn on the appliance after executing the **shutdown** command, you must have physical access to it. For more information, see Powering on the Appliance and Verifying Hardware Operation in the “Cisco Security MARS Hardware Installation and Maintenance Guide 6.X”

⚠ **Caution** The shutdown is immediate and you are not prompted to confirm.

Examples

The following example shuts down the MARS appliance:

```
[pnadmin]$ shutdown
```

Related Commands

Command	Description
predictfsck	Predicts the duration of the file system check that will occur if the Cisco Security MARS is rebooted.

snmpwalk

The **snmpwalk** command loads an SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information.

To use snmpwalk, enter:

snmpwalk [*options*] **agent** [*objectID*]

Syntax Description

no keyword	Displays the command's usage guidelines
options	See Usage Guidelines
agent	
objectID	

Usage Guidelines

snmpwalk command options

```
-h, --help             display this help message
-H                     display configuration file directives understood
-v 1|2c|3              specifies SNMP version to use
-V, --version          display package version number
-c COMMUNITY           set the community string
General communication options
-r RETRIES             set the number of retries
-t TIMEOUT             set the request timeout (in seconds)
Debugging
-d                     dump input/output packets in hexadecimal
-D TOKEN[,...]         turn on debugging output for the specified TOKENs
(ALL gives extremely verbose debugging output)
General options
-m MIB[:...]           load given list of MIBs (ALL loads everything)
-M DIR[:...]           look in given list of directories for MIBs
-P MIBOPTS             Toggle various defaults controlling MIB parsing:
                           u:  allow the use of underlines in MIB symbols
                           c:  disallow the use of "--" to terminate comments
                           d:  save the DESCRIPTIONs of the MIB objects
                           e:  disable errors when MIB symbols conflict
                           w:  enable warnings when MIB symbols conflict
                           W:  enable detailed warnings when MIB symbols conflict
                           R:  replace MIB symbols from latest module
-O OUTOPTS             Toggle various defaults controlling output display:
                           a:  print all strings in ascii format
                           b:  do not break OID indexes down
                           e:  print enums numerically
                           E:  escape quotes in string indices
                           f:  print full OIDs on output
```

```
                          n:  print OIDs numerically
                          q:  quick print for easier parsing
                          Q:  quick print with equal-signs
                          s:  print only last symbolic element of OID
                          S:  print MIB module-id plus last element
                          t:  print timeticks unparsed as numeric integers
                          T:  print human-readable text along with hex strings
                          u:  print OIDs using UCD-style prefix suppression
                          U:  don't print units
                          v:  print values only (not OID = value)
                          x:  print all strings in hex format
                          X:  extended index format
-I INOPTS             Toggle various defaults controlling input parsing:
                          b:  do best/regex matching to find a MIB node
                          r:  do not check values for range/type legality
                          R:  do random access to OID labels
                          h:  don't apply DISPLAY-HINTs
                          u:  top-level OIDs must have '.' prefix (UCD-style)
-C APPOPTS            Set various application specific behaviours:
                          p:  print the number of variables found
                          i:  include given OID in the search range
                          c:  do not check returned OIDs are increasing
```

ssh

To access the SSH client that resides on the appliance, use the **ssh** command.

ssh [-1246AaCfghkMNnqsTtVvXxY] [-b *bind_address***] [-c** *cipher_spec***] [-D** *port***]**
[-e *escape_char***] [-F** *configfile***] [-i** *identity_file***] [-L** *port***:***host***:***hostport***] [-l** *login_name***]**
[-m *mac_spec***] [-o** *option***] [-p** *port***] [-R** *port***:***host***:***hostport***] [-S** *ctl***]**
[*user@hostname* **command]**

Syntax Description

no option or keyword	Displays the command's syntax guidelines.
-A	Enable authentication agent forwarding.
-a	Disable authentication agent forwarding (default).
-c *cipher_spec*	Selects the encryption algorithm.
-e *escape_char*	"none"' = disable (default: ~).
-F *configfile*	Config file (default: ~/.ssh/config).
-f	Fork into background after authentication.
-i *identity_file*	Identity for public key authentication (default: ~/.ssh/identity).
-L *port***:***host***:***hostport*	Forward local port to remote address
-l *login_name*	Log in using this username.
-m *mac_spec*	MAC algorithms for protocol version 2.
-n	Redirect input from /dev/null.
-p portConnect	to this port. Server must be on the same port.
-q Quiet	do not display any warning messages.
-R listen-port:host:port	Forward remote port to local address
-S *ctl*	Specifies the location of a control socket for connection sharing.
-T	Do not allocate a tty.
-t Tty	Allocate a tty even if command is given.
-V	Display version number only.
-v Verbose	Display verbose debugging messages. Multiple -v increases verbosity.
-X	Enable X11 connection forwarding.
-x	Disable X11 connection forwarding (default).

The following options cause ssh to listen for connections on a port, and forward them to the other side by connecting to host:port.

-1	Force protocol version 1.
-2	Force protocol version 2.
-4	Use IPv4 only.
-6	Use IPv6 only.
-b	addr Local IP address.
-C	Enable compression.
-D	port Enable dynamic application-level port forwarding.

-g	Allow remote hosts to connect to forwarded ports.
-N	Do not execute a shell or command.
-o *option*	Process the option as if it was read from a configuration file.
-s	Invoke command (mandatory) as SSH2 subsystem.

Usage Guidelines

For further information on SSH usage, please see SSH Communications Security Corporation documentation at the following URL:

http://www.ssh.com/support/documentation/online/ssh/winhelp/

or open source command references, such as OpenBSD command references:

http://www.openbsd.org/cgi-bin/man.cgi?query=ssh&sektion=1

sslcert

To generate a new self-signed SSL certificate and reboot the JBoss Application Server use the **sslcert** command:

```
sslcert
```

Syntax Description

There are no kewords, arguments or options for this command.

Usage Guidelines

To use this command, you will be prompted to provide the following information:

- The common name of the MARS Appliance
- The name of your organizational unit (OU)
- The name of your organization (O)
- The name of your City or Locality (L)
- The name of your State or Province (SP)
- The two-letter country code for the unit (C)

The **sslcert** command launches an interactive program that collects the information required to generate a certificate. You are prompted to verify that you want to generate a new self-signed certificate. Enter **YES** to begin the interview process that will collect the data required to generate the certificate. Enter **NO** to cancel without generating a new certificate.

With the FIPS PCI Card installed and initialized, you must reboot after executing an **sslcert** command.

Examples

The following command generates a new self-signed certificate:

```
[pnadmin]$ sslcert
Sslcert command will generate a new ssl certificate and restart jboss.
Please type YES if you want to proceed: YES
What is the common name of this device? (CN)
[Unknown]: hostname
What is the name of your organizational unit? (OU)
[Unknown]: test
What is the name of your organization? (O)
[Unknown]: cisco.com
What is the name of your City or Locality? (L)
[Unknown]: San Jose
What is the name of your State or Province? (SP)
[Unknown]: CA
What is the two-letter country code for this unit? (C)
[Unknown]: US
Certificate stored in file <server.cert>
Certificate was added to keystore
Restarting jboss ... OK
```

Related Commands

Command	Description
ssllist	Display a list of ssl certificates

ssllist

Use the ssllist command to display the list of ssl certificates that exist in your keystore.

ssllist

Syntax Description

There are no arguments or keywords for this command.

Command History

Release	Modification
5.2.4	This command was introduced in the 5.2.4 release.
6.0.1	This command was introduced for the MARS 20R, 20, 50, 100E, 100, 200, GCM, and GC.

Examples

The following command lists the SSL certificates of a MARS 200:

```
[pnadmin]$ ssllist

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

server, Jun 18, 2008, trustedCertEntry,
Certificate fingerprint (MD5): D8:13:9B:9A:1F:DB:E8:E6:CB:D1:D8:D3:AF:64:D0:75
```

Related Commands

Command	Description
sslcert	Generates a new self-signed SSL certificate

syslogrelay setcollector

To set, change, or clear the IP address of a host to which the Local Controller forwards the syslog messages it receives, use the **syslogrelay setcollector** command.

syslogrelay {setcollector | unsetcollector} *ip_address*

Command History

Release	Modification
4.3.1	This command was introduced in the 4.X release train.
5.3.1	This command was introduced in the 5.X release train.

Syntax Description

setcollector	Indicates the provided IP address is the collector.
unsetcollector	Clears the provided IP address, and disables the syslog relay feature.
ip_address	Indicates one IP address. You cannot define more than one collector.

Usage Guidelines

The **syslogrelay setcollector** command allows you to specify the IP address of the syslog server to which syslog messages should be forwarded. This command must be used in conjunction with the syslogrelay src command, which designates the reporting devices for which syslog messages should be forwarded.

Examples

The following example specifies that the Local Controller should forward the syslog messages to 192.168.1.25, which is the designated address of the collector.

```
[pnadmin]$ syslogrelay setcollector 192.168.1.25

The following example changes the address of the collector defined in the previous
example.
[pnadmin]$ syslogrelay setcollector 192.168.1.26
syslogrelay setcollector 192.168.1.26
Changing collector ip from 192.168.1.25 to 192.168.1.26. Continue? [y/n]:
```

The following example clears the address of the collector defined in the previous example, effectively disabling the syslog relay feature until a new collector address is set.

```
[pnadmin]$ syslogrelay unsetcollector 192.168.1.26
```

Related Commands

Command	Description
syslogrelay src	Add to, exclude from, or clear the list of IP addresses for which the Local Controller forwards syslog messages to the collector.
syslogrelay list	Displays the list of IP addresses used by the syslogrelay. This list includes the collector, as well as reporting devices in the include and/or exclude lists.

syslogrelay src

To add to, remove from, or clear the lists of sources (reporting devices) for which the Local Controller forwards the syslog messages it receives to the collector, use the **syslogrelay src** command.

syslogrelay src {include | exclude} {ANY | *ip_address1, . . . ip_address10***}**

syslogrelay src reset

Command History

Release	Modification
4.3.1	This command was introduced in the 4.X release train.
5.3.1	This command was introduced in the 5.X release train.

Syntax Description

include	Indicates that syslog messages received by MARS from the listed IP addresses to be relayed to the configured collector.
exclude	Indicates that syslog messages received by MARS from the listed IP addresses should *not* be forwarded to the configured collector.
ANY	Adds all IP addresses to the selected source list.Used in conjunction with either the **include** or **exclude** parameter.
ip_address1, . . . *ip_address10*	Indicates between one and ten IP addresses in a comma separated list. Used in conjunction with the **include** and **exclude** parameters. You can only add up to ten addresses at one time; however, you can use the command repeatedly to add to the list.
reset	Clears the active syslog relay source configuration—both the include and exclude lists. If a syslog relay source is configured, the following prompt appears: `One or more device addresses are currently configured. Proceed further? [yes/no]:` Enter **yes** to clear the source configuration or **no** to cancel.

Usage Guidelines

The **syslogrelay src** command designates the set of reporting devices for which the Local Controller forwards the syslog messages it receives to the collector. You can exclude all addresses, defining the few exceptions for which the syslog messages should be forwarded; or you can enable all addresses, and define the exceptions that should not be forwarded.

The **ANY** token cannot be used simultaneously in both the **include** and **exclude** lists. If the value is set on one list, and you apply it to the other list, it is removed from the first.

The **syslogrelay src include ANY** command indicates that all syslog messages received by MARS be relayed to the configured collector, excepting those that originate from the addresses configured as exclusions. If exclusions are configured, the following prompt appears:

```
One or more device ip addresses are currently excluded. Proceed further? [y/n]:
```

Enter **y** to retain the current exclusions and forward the syslog messages of from all other reporting devices, or enter **n** to cancel.

The **syslogrelay src exclude ANY** command indicates that all syslog messages received by MARS should *not* be forwarded to the configured collector, excepting those that originate from addresses configured as inclusions. If inclusions are configured, the following prompt appears:

```
One or more device ip addresses are currently included. Proceed further? [y/n]:
```

Enter **y** to retain the current inclusions and prevent the forwarding of syslog messages from all other devices, or enter **n** to cancel.

Examples

The following example specifies that the Local Controller should forward the syslog messages it receives from any reporting device to the collector (as long as the source IP address of the message is not in the source exclude list).

```
[pnadmin]$ syslogrelay src include ANY
```

The following example specifies that the Local Controller should not forward the syslog messages it receives from 192.168.1.1 or 192.168.2.1 to the collector.

```
[pnadmin]$ syslogrelay src exclude 192.168.1.1, 192.168.2.1
```

The following example clears the source include and exclude lists of all values:.

```
[pnadmin]$ syslogrelay src reset
One or more device ip addresses are currently configured. Proceed further?[yes/no]: yes
```

Related Commands

Command	Description
syslogrelay setcollector	Set or clear the IP address that identifies the syslog collector to which the Local Controller forwards syslog messages. If the address is cleared, this feature is turned off.
syslogrelay list	List syslog relay configuration. Displays the list of IP addresses used by the syslogrelay. This list includes the collector, as well as reporting devices in the include and/or exclude lists.

syslogrelay list

To display the IP addresses of the reporting devices to which the Local Controller forwards the syslog messages as well as the IP address of the collector to which they are sent, use the **syslogrelay list** command.

syslogrelay list [all | collector | src]

Command History

Release	Modification
4.3.1	This command was introduced in the 4.X release train.
5.3.1	This command was introduced in the 5.X release train.

Syntax Description

-h	Displays usage guidelines
all	(default) Displays the IP address of the collector and the union of those sources on the include list and exclude list.
collector	Displays the IP address of the collector, or destination, of the forwarded messages.
src	Displays the IP addresses of the sources on the include list and exclude list.

Usage Guidelines

Using the **syslogrelay list** command, you can verify the list of addresses in the include and exclude lists. If a reporting device device appears in the include list, the Local Controller forwards any syslog messages that it receives from that device to the syslog collector. The exclude list identifies the IP addresses for which the Local Controller does not forward the syslog messages. The collector identifies the IP address to which the specified syslog messages are forwarded. This address represents a syslog server or other collector as defined in *RFC 3164: The BSD syslog Protocol*.

If the collector address is not set, the syslogrelay feature is disabled.

Examples

The following example displays the t syslog relay configuration.

```
[pnadmin]$ syslogrelay list all
[Collector]
192.168.1.1

[Inclusions]
ANY

[Exclusions]
192.168.2.1
182.168.3.1
```

Related Commands

Command	Description
syslogrelay setcollector	Set or clear the IP address that identifies the syslog collector to which the Local Controller forwards syslog messages. If the address is cleared, this feature is turned off.
syslogrelay src	Add to, exclude from, or clear the list of IP addresses for which the Local Controller forwards syslog messages to the collector.

sysstatus

To view the current CPU activities, enter:

sysstatus -hvbcisqS -d delay -p *pid* **-n** *iterations*

Syntax Description

no keyword	Displays the current CPU activities.
-h	Displays the detailed command's usage guidelines.
-d	Specifies the delay between screen updates. You can change this delay using the -s interactive command.
-p	Monitors only those processes with the given process id. This flag can be given up to twenty times. This option is not available interactively.
-q	This causes sysstatus to refresh without any delay.
-S	Specifies cumulative mode, where each process is listed with the CPU time it has spent. It also lists the CPU time of the dead children for each process.
-s	Tells sysstatus to run in secure mode. This option disables the potentially dangerous interactive commands.
-i	Start sysstatus ignoring any idle or zombie processes.
	-C Display total CPU states in addition to individual CPUs. This option only affects SMP systems.
-c	Display the command line instead of the command name only. The default behavior has been changed as this seems to be more useful.
-n	Number of iterations. Update the display this number of times and then exit.
-b	Batch mode. Useful for copying output from sysstatus to a file. In this mode, sysstatus does not accept command line input. It runs until it reaches the number of iterations specified by the n option or until killed. Output is plain text suitable for display on a dumb terminal.

Usage Guidelines

The **sysstatus** command is a system-defined alias for the Linux **top** command, which displays and updates information about the top CPU processes. It provides a real-time view of the processor activity. It lists the most CPU-intensive tasks on the system, and can provide an interactive interface for manipulating processes. It can sort the tasks by CPU usage, memory usage, and runtime.

If you execute the command and you do not select the batch mode option, you are running in an interactive environment. In this environment, you can interact with the output as follows:

- Press **H** or **?** to get the list of interactive commands.
- Press the **space** key to refresh the data immediately.
- Press **Ctrl+L** to erase and redraw the screen.
- Press **K** to kill a specific process ID (pid).
- Press **Q** to quit viewing the real-time data and return to the command prompt.
- Press **Ctrl+C** to break the batch mode display.

- Press **I** to toggle ignoring idle and zombie processes.
- Press **N** or **#** to specify the number of processes to display on the screen. The value of zero (0) restores the default, which is the number of processes that fit on the screen.
- Press **S** to toggles the cumulative mode, the equivalent of -S, that includes a process's defunct children as part of the CPU times.
- Press **f** or **F** to add fields or remove fields from the display.
- Press **o** or **O** to change the order of the displayed fields.
- Press **L** to toggle the display of load average and uptime information.
- Press **M** to toggle the display of memory information.
- Press **T** to toggle the display of processes and CPU states information.
- Press **C** to toggle the display of command name or full command line.
- Press **N** to sort the tasks numerically by pid.
- Press **A** to sort the tasks by age (newest first).
- Press **P** to sort the tasks by CPU usage (default).
- Press **M** to sort the tasks by resident memory usage.
- Press **T** to sort the tasks by time/cumulative time.

tcpdump

Tcpdump prints to the console the headers of packets on a network interface that match the boolean *expression*. Exit with **Ctrl+C.**

tcpdump [**-adeflnNOpqRStuvxX**] [**-c** *count*] [**-i** *interface*] [**-s** *snaplen*] [**-T** *type*] [**-U** *user*] [*expression*]

Syntax Description

No option or keyword	Dumps all headers of packets on the network interface to the terminal in real time.
-c *count*	Exit after receiving *count* number of packets.
-i *interface*	Identifies the interface to sniff.
-s *snaplen*	Snarf *snaplen* bytes of data from each packet rather than the default of 68.
-T *type*	Force packets selected by *expression* to be interpreted the specified *type*. Types are: • cnfp (Cisco NetFlow protocol) • rpc (Remote Procedure Call) • rtp (Real-Time Applications protocol) • rtcp (Real-Time Applications control protocol) • snmp (Simple Network Management Protocol) • vat (Visual Audio Tool) • wb (distributed White Board).
-U *user*	Drops root privileges and changes user ID to user and group ID to the primary group of user.
expression	Species which packets are dumped. If no *expression* is specified, all packets are dumped. Otherwise, only packets for which expression is ‘true’ will be dumped.
-h	Displays the detailed command’s usage guidelines.

Usage Guidelines

Ctrl+C exists the tcpdump screen.

Note For more information on this command and its use, please refer to a Linux command reference or man page.

telnet

The **telnet** command is used to communicate with another host using the TELNET protocol. In this mode, it accepts and executes the commands listed below. If it is invoked with arguments, it performs an open command with those arguments.

telnet [**-8**] [**-E**] [**-L**] [**-S** *tos*] [**-a**] [**-c**] [**-d**] [**-e** *char*] [**-l** *user*] [**-n** *tracefile*] [**-b** *hostalias*] [**-r**] [*hostname* [*port*]]

Syntax Description

no option or keyword	Displays command usage.
-8	Specifies an 8-bit data path, which forces telnet to attempt to negotiate the BINARY option on both input and output.
-E	Stops any character from being recognized as an escape character.
-L	Specifies an 8-bit data path on output. This causes the BINARY option to be negotiated on output.
-a	Attempt automatic login. The name used is that of the current user.
-b *hostalias*	Uses bind on the local socket to bind it to an aliased address (see ifconfig and the “alias” specifier) or to the address of another interface than the one naturally chosen by connect. This can be useful when connecting to services which use IP addresses for authentication and reconfiguration of the server is undesirable (or impossible).
-c	Disables the reading of the user's .telnetrc file.
-d	Sets the initial value of the debug toggle to TRUE.
-e *escapechar*	Sets the initial telnet escape character to escapechar. If escapechar is omitted, there will be no escape character.
-l *user*	When a host connects to the remote system, if the remote system understands the ENVIRON option, the user will be sent to the remote system as the value for the variable USER. This option implies the -a option. This option may also be used with the open command.
-n *tracefile*	Opens tracefile for recording trace information.
-r	Specifies a user interface similar to rlogin. In this mode, the escape character is set to the tilde (~) character, unless modified by the -e option.
hostname	Indicates the official name, an alias, or the Internet address of a remote host.
port	Indicates a port number (address of an application) used to connect on the remote host. If a number is not specified, the default telnet port is used.

Usage Guidelines

For more information on this command and its use, please refer to a Linux command reference or man page.

time

To display the current time, enter:

time

To set the time to 11:15 p.m., enter:

time [*hh***:***mm***:***ss*]

Syntax Description

hh:mm:ss Identifies the time in *hh*:*mm*:*ss* format, where *hh* is 01-24, *mm* is 00-59 and *ss* is 00-59.

Usage Guidelines

Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than one half hour, you should restart your appliance to ensure that all processes synchronize using the new time.

Examples

The following example displays the current time of a MARS 200:

```
[pnadmin]$ time
17:04:40
```

The following example changes the time to 11:15 p.m., enter:

```
[pnadmin]$ timezone 23:15:00
[pnadmin]$ time
23:15:00
```

Related Commands

Command	Description
ntp	identifies the primary and secondary NTP server with which the appliance should synchronize.
timezone	Displays and configures the MARS timezone setting

timezone

To display the current timezone setting, enter:

timezone

To set a new timezone, enter:

timezone set

When configuring a Global Controller\Local Controller hierarchy, you should ensure that all the Local Controllers are set to the same timezone as the reporting devices that they are monitoring.

Note Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than 30 minutes, you should restart your appliance to ensure that all processes synchronize using the new time.

Syntax Description

set Displays a menu system that allows you to select the appropriate timeszone based on continent/country/region or using the POSIX TZ format.

Examples

The following example displays the current time of a MARS 200:

```
[pnadmin]$ timezone
17:04:40
PDT -0700
```

The following example sets the timezone to Pacific time:

```
[[pnadmin]$ timezone set
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 2
Please select a country.
 1) Anguilla              27) Honduras
 2) Antigua & Barbuda     28) Jamaica
 3) Argentina             29) Martinique
 4) Aruba                 30) Mexico
 5) Bahamas               31) Montserrat
 6) Barbados              32) Netherlands Antilles
 7) Belize                33) Nicaragua
 8) Bolivia               34) Panama
 9) Brazil                35) Paraguay
10) Canada                36) Peru
11) Cayman Islands        37) Puerto Rico
```

```
12) Chile                    38) St Barthelemy
13) Colombia                 39) St Kitts & Nevis
14) Costa Rica               40) St Lucia
15) Cuba                     41) St Martin (French part)
16) Dominica                 42) St Pierre & Miquelon
17) Dominican Republic       43) St Vincent
18) Ecuador                  44) Suriname
19) El Salvador              45) Trinidad & Tobago
20) French Guiana            46) Turks & Caicos Is
21) Greenland                47) United States
22) Grenada                  48) Uruguay
23) Guadeloupe               49) Venezuela
24) Guatemala                50) Virgin Islands (UK)
25) Guyana                   51) Virgin Islands (US)
26) Haiti
#? 47
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Starke County
 8) Eastern Time - Indiana - Pulaski County
 9) Eastern Time - Indiana - Crawford County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Pike County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21


The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Fri Apr 27 17:12:09 PDT 2008.
Universal Time is now:  Sat Apr 28 00:12:09 UTC 2008.
Is the above information OK?
1) Yes
2) No
#? 1) Yes
2) No
#? 1
Restarting jboss:  OK
Stopping SuperV:  OK
Starting SuperV:  OK
```

Related Commands

Command	Description
ntp	Specifies the primary and secondary NTP servers with which the appliance should synchronize.
time	Displays and configures the MARS timeclock

traceroute

To display the network route that packets take to reach a specified host, enter:

traceroute [-dFInrvx] [-**g** *gateway*] [-**i** *iface*] [-**f** *first_ttl*]
[-**m** *max_ttl*] [-**p** *port*] [-**q** nqueries] [-**s** *src_addr*] [-**t** *tos*]
[-**w** *waittime*] [-**z** *pausemsecs*] **host** [*packetlen*]

Syntax Description

no keyword or option	Displays the command's usage guidelines.
-**g** *gateway*	
-**i** *iface*	
-**f** *first_ttl*	
-**m** *max_ttl*]	
-**p** *port*	
-**q** nqueries	
-**s** *src_addr*	
-**t** *tos*	
-**w** *waittime*	
-**z** *pausemsecs*	
host [*packetlen*]	
-d	
-F	
-I	
-n	
-r	
-v	
-x	

Usage Guidelines

Traces the route that IP packets take from the MARS appliance to another host on a network by listing the intermediate gateways that the packet traverses to reach the host.

Traceroute displays the IP address and hostname (if possible) of the gateways along the route taken by the packets. Traceroute is used as a network debugging tool. If you are having network connectivity problems, traceroute will help you diagnose where the trouble might exist along the route.

Use the traceroute command to discover the routes that packets take, when traveling to their destination.Specify a hostname or an IP address as an argument to this command.

This command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute 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 a "time-exceeded" error message. The trace command sends three probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet may result in one of the following messages:

A "time-exceeded" error message - This indicates that an intermediate router has seen and discarded the probe, when the TTL was decremented to zero.

A "destination-unreachable" error message - This indicates that the destination node has received the probe and discarded it because it did not have a route to the destination.

An "*" - If a timeout occurs before a response comes in, an asterisk (*) is displayed.

An "invalid-port" error message - This indicates that the destination node received the trace message, which was addressed to an invalid port.

The traceroute command terminates when the destination is reached, when the maximum TTL is exceeded, or when the user interrupts the trace with the <Ctrl>-<Shift>-6 sequence.

unlock

Use the **unlock** command to restore access to the MARS Appliance GUI for all or specified user accounts after login failures.

unlock {**-a** }| {{**-l** | **-g** | **-b** } *login_name*}

Command History

Release	Modification
4.3.1/5.3.1	This command was introduced.

Syntax Description

-a	Unlocks all accounts on the MARS Appliance.
-l	Unlocks the local account for the specified login name.
-g	Unlocks the global account for the specified login name.
-b	Unlocks global and local accounts for the specified login name.
login_name	Specifies the login name of the account to be unlocked.

Usage Guidelines

For both Local or AAA authentication methods, GUI access is prevented (locked) for an account upon login failure, which occurs when a specified number of incorrect password entries are made for a single login name. The administrator GUI access can be locked like any other account.

The CLI access through the console or through SSH is never locked. The **unlock** CLI command can unlock GUI access for some or all accounts.

Unlocking is not replicated through Global Controller–Local Controller communications, it applies only to the local appliance. An account locked on a Global Controller does not replicate the locked status to global accounts on Local Controllers. A global account locked on two different appliances must be unlocked manually on each appliance.

For more information on account locking and login failure, see the section, “Information About Authenticating MARS User Accounts with External AAA Servers” at the following URL: http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/authen.html#wp431897

Examples

The following example unlocks GUI access for a local account with the login name bleistiftansatz:

```
[pnadmin]$ unlock -l bleistiftansatz
```

Related Commands

Command	Description
passwd	Changes the password of the system administrative account (pnadmin) associated with the appliance.

version

To display the version of the MARS software running on the appliance, use the **version** command.

version

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

The version number appears in the following format: *major.minor.patch* (*build no.*) *data package*

The data and binary upgrade can be packaged and upgraded separately.

Examples

The following command displays the software version running on a MARS 200:

```
[pnadmin]$ version
6.0.1 (2980) 30
```

INDEX