

Cisco Prime Network Analysis Module
Command Reference Guide

Versions 5.1(2), 5.1(3), 6.0(1), 6.0(2), and 6.1(1)
July 2014

**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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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 Prime Network Analysis Module Command Reference Guide

© 2012-2014 Cisco Systems, Inc. All rights reserved.

Contents

[About This Guide 9](#_Toc378026319)

[1: Command Line Interface 12](#_Toc378026320)

[2: NAM CLI Commands: application - device waas 16](#_Toc378026321)

[application 20](#_Toc378026322)

[application group 22](#_Toc378026323)

[audit-trail enable 24](#_Toc378026324)

[autocreate-data-source 25](#_Toc378026325)

[cdp enable 26](#_Toc378026326)

[cdp hold-time 29](#_Toc378026327)

[cdp interval 30](#_Toc378026328)

[classification-mode default 31](#_Toc378026329)

[classification-mode deep-inspect 32](#_Toc378026330)

[clear access log 33](#_Toc378026331)

[clear captured-data-files 35](#_Toc378026332)

[clear monitoring-data 37](#_Toc378026333)

[clear system-alerts 38](#_Toc378026334)

[clear system-passwords 39](#_Toc378026335)

[clock set 41](#_Toc378026336)

[config clear 42](#_Toc378026337)

[config network 44](#_Toc378026338)

[config upload 46](#_Toc378026339)

[coredump 48](#_Toc378026340)

[data-source erspan 49](#_Toc378026341)

[data-source netflow 51](#_Toc378026342)

[data-source pa 53](#_Toc378026343)

[data-source waas 55](#_Toc378026344)

[debug log disable 57](#_Toc378026345)

[debug log enable 58](#_Toc378026346)

[debug log level 59](#_Toc378026347)

[debug log metric-engine 61](#_Toc378026348)

[debug log reset 62](#_Toc378026349)

[device erspan 63](#_Toc378026350)

[device netflow 64](#_Toc378026351)

[device waas 66](#_Toc378026352)

[3: NAM CLI Commands: email – managed-device community 67](#_Toc378026353)

[email 69](#_Toc378026354)

[entity alias 71](#_Toc378026355)

[entity assetid 72](#_Toc378026356)

[exit 73](#_Toc378026357)

[exsession 74](#_Toc378026358)

[ftp 76](#_Toc378026359)

[help 78](#_Toc378026360)

[ip address 79](#_Toc378026361)

[ip broadcast 81](#_Toc378026362)

[ip domain 82](#_Toc378026363)

[ip gateway 83](#_Toc378026364)

[ip host 84](#_Toc378026365)

[ip hosts add 85](#_Toc378026366)

[ip hosts delete 87](#_Toc378026367)

[ip http port 88](#_Toc378026368)

[ip http secure generate 90](#_Toc378026369)

[ip http secure install certificate 91](#_Toc378026370)

[ip http secure port 92](#_Toc378026371)

[ip http secure server 93](#_Toc378026372)

[ip http server 94](#_Toc378026373)

[ip http tacacs+ 95](#_Toc378026374)

[ip interface 97](#_Toc378026375)

[ip nameserver 98](#_Toc378026376)

[license install 99](#_Toc378026377)

[logout 100](#_Toc378026378)

[managed-device address 101](#_Toc378026379)

[managed-device community 102](#_Toc378026380)

[4: NAM CLI Commands: metric export host - show certificate request 103](#_Toc378026381)

[metric export host 106](#_Toc378026382)

[metric export non-waas traffic 107](#_Toc378026383)

[monitor data-aggr-intv 108](#_Toc378026384)

[monitor nbar 110](#_Toc378026385)

[monitor protocol encapsulation 111](#_Toc378026386)

[monitor rtp-stream enable 112](#_Toc378026387)

[monitor rtp-stream filter 113](#_Toc378026388)

[monitor rtp-stream threshold 114](#_Toc378026389)

[monitor urlcollection 116](#_Toc378026390)

[monitor urlfilter 118](#_Toc378026391)

[mtrace-clear, mtrace-show, mtrace-start, mtrace-stop, mtrace-upload 120](#_Toc378026392)

[netflow input port 121](#_Toc378026393)

[nslookup 122](#_Toc378026394)

[password 123](#_Toc378026395)

[password strong-policy 124](#_Toc378026396)

[patch 125](#_Toc378026397)

[pid-sn 127](#_Toc378026398)

[ping 128](#_Toc378026399)

[ping6 129](#_Toc378026400)

[preferences 132](#_Toc378026401)

[protocol esp-null-heuristic 134](#_Toc378026402)

[reboot 135](#_Toc378026403)

[reboot -helper 136](#_Toc378026404)

[reboot -golden 137](#_Toc378026405)

[remote-storage 138](#_Toc378026406)

[remote-storage fcoe 139](#_Toc378026407)

[remote-storage iscsi 141](#_Toc378026408)

[remote-storage sas 143](#_Toc378026409)

[remove corefiles 145](#_Toc378026410)

[rise-nam enable / disable 146](#_Toc378026411)

[rmwebusers 147](#_Toc378026412)

[secure-clear all 148](#_Toc378026413)

[show access-log 149](#_Toc378026414)

[show application app-id 150](#_Toc378026415)

[show application eng-id 151](#_Toc378026416)

[show application group 152](#_Toc378026417)

[show audit-trail 155](#_Toc378026418)

[show autocreate-data-source 156](#_Toc378026419)

[show cdb 157](#_Toc378026420)

[show cdp settings 160](#_Toc378026421)

[show certificate 161](#_Toc378026422)

[show certificate-request 162](#_Toc378026423)

[5: NAM CLI Commands: show clock details - show monitor urlfilter 163](#_Toc378026424)

[show classification-settings 164](#_Toc378026425)

[show clock details 166](#_Toc378026426)

[show configuration 167](#_Toc378026427)

[show corefiles 169](#_Toc378026428)

[show counters 170](#_Toc378026429)

[show cpu 171](#_Toc378026430)

[show data-source 172](#_Toc378026431)

[show date 173](#_Toc378026432)

[show debug log-levels 174](#_Toc378026433)

[show debug messages 176](#_Toc378026434)

[show debug metric-engine 177](#_Toc378026435)

[show debug online-diag-stats 178](#_Toc378026436)

[show debug rise-messages 179](#_Toc378026437)

[show decode-log 180](#_Toc378026438)

[show device 181](#_Toc378026439)

[show email 182](#_Toc378026440)

[show entity 183](#_Toc378026441)

[show ftp 184](#_Toc378026442)

[show hosts 185](#_Toc378026443)

[show interface management-port 186](#_Toc378026444)

[show internal resources monitoring 187](#_Toc378026445)

[show inventory 189](#_Toc378026446)

[show ip 190](#_Toc378026447)

[show license 192](#_Toc378026448)

[show local-storage all 193](#_Toc378026449)

[show local-storage physical 199](#_Toc378026450)

[show local-storage progress 204](#_Toc378026451)

[show local-storage virtual 205](#_Toc378026452)

[show log config 207](#_Toc378026453)

[show log patch 208](#_Toc378026454)

[show log report 209](#_Toc378026455)

[show log upgrade 210](#_Toc378026456)

[show memory 211](#_Toc378026457)

[show metric export 212](#_Toc378026458)

[show monitor protocol encapsulation 213](#_Toc378026459)

[show monitor protocol all 214](#_Toc378026460)

[show monitor rtp-stream 215](#_Toc378026461)

[show monitor rtp-stream filter 216](#_Toc378026462)

[show monitor urlcollection 217](#_Toc378026463)

[show monitor urlfilter 218](#_Toc378026464)

[6: NAM CLI Commands: show password strong-policy - web user 219](#_Toc378026465)

[show password strong-policy 221](#_Toc378026466)

[show patches 222](#_Toc378026467)

[show pkt-drop counters 223](#_Toc378026468)

[show preferences 224](#_Toc378026469)

[show protocol-feature 225](#_Toc378026470)

[show remote-storage 226](#_Toc378026471)

[show rxcounters 227](#_Toc378026472)

[show snmp 228](#_Toc378026473)

[show syslog-settings 229](#_Toc378026474)

[show system-alerts 230](#_Toc378026475)

[show tech-support 231](#_Toc378026476)

[show time 232](#_Toc378026477)

[show time ptp 233](#_Toc378026478)

[show trap-dest 234](#_Toc378026479)

[show top-memory-users 236](#_Toc378026480)

[show version 237](#_Toc378026481)

[show waas data-source 238](#_Toc378026482)

[show waas device 239](#_Toc378026483)

[show waas server filter 240](#_Toc378026484)

[show web-publication 241](#_Toc378026485)

[show web-user 242](#_Toc378026486)

[shutdown 243](#_Toc378026487)

[snmp 244](#_Toc378026488)

[syslog 245](#_Toc378026489)

[syslog remote-server 246](#_Toc378026490)

[terminal 248](#_Toc378026491)

[time 249](#_Toc378026492)

[traceroute 251](#_Toc378026493)

[traceroute6 253](#_Toc378026494)

[trap-dest 254](#_Toc378026495)

[upgrade 256](#_Toc378026496)

[waas export server-filter-list 257](#_Toc378026497)

[waas import server-filter-list 258](#_Toc378026498)

[waas server filter 259](#_Toc378026499)

[web-publication 260](#_Toc378026500)

[web-user 262](#_Toc378026501)

Appendix A
NAM Maintenance Partition CLI 264

Appendix B
Acronyms
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 266

About This Guide
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­­­­­­­­­­­­­­­­­­­­­­­­­

This guide provides information for using the Cisco Prime Network Analysis Module (NAM) software command line interface (CLI).

## Audience

This guide is designed for network administrators who are responsible for setting up and configuring Cisco Prime NAMs to monitor traffic and diagnose emerging problems on network segments. As a network administrator, you should be familiar with:

* Basic concepts and terminology used in internetworking.
* Network topology and protocols.
* Basic UNIX commands or basic Windows operations.

## How This Guide is Organized

This guide is organized as follows:

|  |  |  |
| --- | --- | --- |
| Chapter | Title | Description |
| Chapter 1 | 1: Command Line Interface\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Describes how to log into the NAM and gives information about the two CLI command modes (the command mode and subcommand mode) and information about NAM CLI edit and create modes. |
| Chapter 2 | 2: NAM CLI Commands: application - device waas\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Lists CLI commands alphabetically and provides detailed information about the commands. |
| Chapter 3 | 3: NAM CLI Commands: email – managed-device community\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Lists CLI commands alphabetically and provides detailed information about the commands. |
| Chapter 4 | [NAM CLI Commands: metric export host - show certificate request](#_Toc330561987)  | Lists CLI commands alphabetically and provides detailed information about the commands. |
| Chapter 5 | 5: NAM CLI Commands: show classification-settings to show monitor urlfilter | Lists CLI commands alphabetically and provides detailed information about the commands. |
| Chapter 6  | 6: NAM CLI Commands: show password strong-policy - web user\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Lists CLI commands alphabetically and provides detailed information about the commands. |
| Appendix A | Appendix ANAM Maintenance Partition CLI\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Lists the NAM maintenance partition commands.  |
| Appendix B | Appendix BAcronyms\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  | Defines the acronyms used in this guide.  |

This document uses the following conventions:

|  |  |
| --- | --- |
| Item | Convention |
| Commands and keywords | boldfacefont |
| Variables for which you supply values | italicfont |
| Displayed session and system information | screen font |
| Information you enter | boldface screen font |
| Variables you enter | italic screen font |
| Menu items and button names | boldface font |

* Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.
*  Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.
*  This symbol means danger. You are in a situation that could cause bodily injury.

## Product Documentation

For more information about the documentation set for this product or other documentation including supported platforms, see the following URL:

[http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd\_products\_support\_series\_home.
html](http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, sees 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.

# 1: Command Line Interface\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter provides information for understanding and using the Cisco Prime Network Analysis Module Command Reference Guide software by using the command-line interface (CLI). This chapter includes the following sections:

* Logging into the NAM
* Getting Help
* Command Mode
* Subcommand Mode
* Creation and Edit Modes
* NAM Supported Platforms

For an overview of your platform-specific configuration, see Cisco.com.

## Logging into the NAM

Initial configuration or reconfiguration of network settings may require access to the console. Depending on your platform, you may access the console differently.

* For NAM appliances, access the console using a physical keyboard and monitor or by hooking up a cable to the serial port on NAM 2200 appliances or CIMC management port on NAM 2300 appliances.
* For NAM-3 on Cat6K and NAM-NX1 on Nexus 7K, access the console connection using switch CLI
* For NAM on SM-SRE and NME-NAM, access a console connection using the router cli.
* For NAM on Nexus or NAM on WAAS installations, access a console through the host appliance cli.

The example given below gives instructions on how to access the NAM console on the NAM-1, NAM-2, or NAM-3 platform. For more details, see the installation guide for each platform.

There are two levels of access on the Network Analysis Module, each with different privileges:

* Guest—Read-only access (default password is guest). This account has been removed since NAM 6.0(1) due to security requirements.
* Root—Full read-write access (default password is root)
* The root account uses the **#** prompt; the guest account uses the **>** prompt.

This example opens a session to log into the NAM-1, -2, or -3, and NAM-NX1 consoles:

* Log into the console using the Telnet connection or the console port connection.
* Establish a console session with the NAM at the CLI prompt, using the session/attach command. For example:

Cisco IOS Software:

switch> session slot 4 processor 1

The default escape character is Ctrl-^, then x.

You can also type 'exit' at the remote prompt to end the session

Trying 209.165.200.225 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-3)

login:

Catalyst Operating System Software:

switch> session 3

Trying NAM-3...

Connected to NAM-3.

Escape character is '^]'.

Cisco Network Analysis Module (WS-SVC-NAM-3)

login:

**Cisco Nexus Operating System (NX-OS) Software:**

namlab-n7k-7# attach module 3 p 1

Attaching to module 3 proc-1...

telnet 127.1.4.25...

To exit type 'exit', to abort type 'Ctrl-^' or 'Ctrl+Shift+6'

Telnet escape character is '^^'.

Trying 127.1.4.25...

Connected to 127.1.4.25.

Escape character is '^^'.

Cisco Prime Network Analysis Module

n7k7-mod9.cisco.com login:

* Log into the NAM by typing **root** to log in as the root user or **guest** to log in as a guest user at the login prompt.

login: **root**

* At the password prompt, enter the password for the account. The default password for the root account is “root,” and the default password for the guest account is “guest.”

Password:

After a successful login, the command-line prompt appears with information on the module and copyright. For example, the Cisco Catalyst 6500 series displays as follows:

Cisco Catalyst 6500 Series Network Analysis Module (WS-SVC-NAM-3-K9) Console, 5.0(1T.45)

Copyright (c) 1999-2011 by Cisco Systems, Inc.

nam.domain.com#

* After you log in for the first time, you will be asked to change the default password.

### Changing the Default Password

To change the password, follow these steps while you are logged into the root account on the NAM:

* Enter this command as follows:

root@localhost# password username

To change the root password, make a Telnet connection to the NAM and then use the password root command.

To change the guest password, make a Telnet connection to the NAM and then use the password guest command.

* Enter the new password as follows:

Changing password for user root

New UNIX password:

* Enter the new password again as follows:

Retype new UNIX password:

passwd: all authentication tokens updated successfully

This example shows how to set the password for the root account:

root@localhost# password root

Changing password for user root

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully

## Getting Help

When you have successfully logged in, enter a ? and press Return or enter the **help** command for a list of commands used to configure the NAM. For example:

Cisco Catalyst 6500 Series Network Analysis Module (WS-SVC-NAM-3-K9) Console, 5.0(1T.45)

Copyright (c) 1999-2012 by Cisco Systems, Inc.

nam.domain.com# help

? - display help

application - configure an application [group]

audit-trail - enable logging into Web GUI and CLI accesses

autocreate-data-source - enable data source autocreation feature

clear - clear access log / system alerts

...

## Command Mode

The Cisco Prime Network Analysis Module provides a configurable command mode accessible when you log into the NAM as “root.” Certain commands enter into a subcommand mode. In all command and subcommand modes, the asterisk (\*) specifies that the subcommand is mandatory.

## Subcommand Mode

Some commands enter into a subcommand mode, which provides additional configuration commands that you can use in that mode. For example:

root@nam.domain.com# time

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam.domain.com(sub-time)#

When you have entered the subcommand mode, type a ? or enter the **help** command for a list of commands available in that subcommand mode. For example:

root@nam.domain.com(sub-time)# ?

? - display help

cancel - discard changes and exit from subcommand mode

exit - exit from subcommand mode

help - display help

sync - synchronize NAM system time with switch, ntp, or local clock

zone - configure time zone at the NAM

root@nam.domain.com(sub-time)#

* For the commands that enter into a subcommand mode, the actual configuration is completed only when you enter the **exit** command.

## Creation and Edit Modes

Some commands run in a creation mode and an edit mode, which alternate depending on whether you are creating or changing (editing) a configuration.

## NAM Supported Platforms

For login details to the NAM supported platforms in this release, see your platform-specific installation guide at Cisco.com.

# 2: NAM CLI Commands: application - device waas\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter contains an alphabetical listing of the commands unique to the Cisco platforms that support the 5.1(2), 5.1(3), 6.0(1), 6.0(2) and 6.1(1) releases. For information on the supported platforms, see the Cisco Prime Network Analysis Module Release Notes.

For information on Cisco IOS commands to configure your specific hardware platform, see Related Documentation.

For ease of use, NAM CLI Commands, are divided into five different chapters:

* 2: NAM CLI Commands:
application - device waas
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (this chapter)
* 3: NAM CLI Commands:
email – managed-device community
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* 4: NAM CLI Commands:
metric export host - show certificate request
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* 5: NAM CLI Commands:
show classification-settings to show monitor urlfilter
* 6: NAM CLI Commands:
show password strong-policy - web user
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter describes the following commands:

* application
* application group
* audit-trail enable
* autocreate-data-source
* **Error! Reference source not found.**
* cdp hold-time
* cdp interval
* classification-mode default
* To use default NAM packet classification, use the classification-mode default command. This command is introduced in NAM 6.0(1).

Classification-mode default

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to use default NAM packet classification:

root@nam.localdomain# classification-mode default

Default classification is already in effect

# classification-mode deep-inspect

To use deep packet inspection (EFT feature), use the classification-mode deep-inspect command. This command was introduced in NAM 6.0(1).

Classification-mode deep-inspect

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to use deep packet inspection:

root@nam.localdomain# classification-mode deep-inspect

This operaton will restart NAM services for the changes to take effect.

Do you wish to continue? (y/n) [n]:

* clear access log
* clear captured-data-files
* clear monitoring-data
* clear system-alerts
* clear system-passwords
* clock set
* config clear
* config network
* config upload
* coredump
* data-source erspan
* data-source netflow
* data-source pa
* data-source waas
* debug log disable
* debug log enable
* debug log level
* debug log metric-engine
* debug log reset
* device erspan
* device netflow
* device waas

# application

To create an application, use the application command. To remove an application match, use the no application command.

**application**

**no application**

This command has no default settings.

Command mode

When you enter the application submode, the following commands are available:

* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the exit command section.
* **help**—Displays help and keeps you in the application subcommand mode; see the “help” command section.
* match—Specifies an application match with subcommands below as of NAM 6.1(1)
	+ server – configure a server ip to match
	+ tcp – configure a tcp port to match
	+ udp – confiture a udp port to match
	+ url – configure an http url regular expression match
		- host – specify the http url host part
		- path – specify the http url path/host part
* name string—Sets the application name. This is a mandatory field.

This example shows how to create an application:

root@NAM# application

new application (app tag 268435459)

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@NAM(sub-application)# ?

? - display help

cancel - discard changes and exit from subcommand mode

exit - exit from the subcommand mode

help - display help

match - specify an application match

name - enter the application name (\*)

no - remove an application match

(\*) - denotes a mandatory field for this configuration.

root@NAM(sub-application)#

# application group

To enter the application group submode and define an application group, use the application group command. To remove an application group, use the **no** form of this command.

application **group**

no application **group** group-name

|  |  |
| --- | --- |
| group-name | Application group name. |

This command has no default settings.

Command mode

When you enter the application group submode, the following commands are available:

* add protocol-specifier—Adds a protocol to the group. You only can add one protocol to a group at a time (for example, HTTPS). This command allows you to group statistics for more than one specified protocol into one counter.

To add two or more protocols to an application group, repeat the add command for each protocol. The protocols are added only when you exit application group subcommand mode.

* **cancel**—Discards changes and exits from the subcommand mode.
* delete protocol-specifier—Removes a protocol from the group. You only can remove one protocol from a group at a time.

To remove two or more existing protocols from an existing application group, repeat the delete command for each protocol. The protocol is removed only when you exit the application group subcommand mode.

* **exit**—Saves changes and exits from the subcommand mode.
* **help**—Displays help and keeps you in the application group subcommand mode.
* name string—Sets the application group name.

You must provide protocol specifiers in the add or delete parameters, or both the add and delete parameters.

This example shows how to create an application group named appGrpSample with two protocols in the group:

root@NAM# application group

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@NAM(sub-application-group)# ?

? - display help

add - add a protocol to the group (\*)

cancel - discard changes and exit from subcommand mode

delete - remove a protocol from the group (\*)

exit - exit from subcommand mode

help - display help

name - set application group name (\*)

(\*) - denotes a mandatory field for this configuration.

root@NAM(sub-application-group)# add 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.68.4.0.1.0.0

root@NAM(sub-application-group)# add 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.4.60.4.0.1.0.0

root@NAM(sub-application-group)# name appGrpSample

root@NAM(sub-application-group)# exit

Sucessfully create application group appGrpSample.

root@NAM#

root@NAM#

root@NAM# show application group appGrpSample

Application Group: appGrpSample

 Number of Protocols: 2

 - w-ether2.ip.tcp.tcp-836

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.68.4.0.1.0.0

 - w-ether2.ip.udp.udp-1084

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.4.60.4.0.1.0.0

root@NAM#

**show application group**

# audit-trail enable

To enable and audit trail of GUI and CLI accesses, use the audit-trail enable command. To disable audit trail of GUI and CLI accesses, use the no form of this command.

audit-trail enable

no audit-trail enable

Audit trail of the CLI and GUI accesses is enabled.

Command mode

This example shows how to enable an audit trail for GUI and CLI accesses:

root@hostname.cisco.com# audit-trail enable

show audit-trail

# autocreate-data-source

To enable autocreation of the data-source, use the **autocreate data-source** command. To disable autocreation of data-sources on NAM, use the no form of this command.

autocreate data-source

no autocreate data-source

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to enable autocreation of data-sources:

root@nam235Cat6k.cisco.com# autocreate-data-source ?

erspan - enable autocreation of ERSPAN data sources

netflow - enable autocreation of NDE data sources

waas - enable autocreation of WAAS data sources

waas-client - enable autocreation of WAAS Client data sources

waas-client-wan - enable autocreation of WAAS Client WAN data sources

waas-passthru - enable autocreation of WAAS Passthru data sources

waas-passthru-export - enable Passthru export on autocreated WAAS devices

waas-server - enable autocreation of WAAS Server data sources

waas-server-wan - enable autocreation of WAAS Server WAN data sources

root@nam235Cat6k.cisco.com# autocreate-data-source

# cdp enable

To enable the Cisco Discovery Protocol (CDP) on the NME-NAM, use the cdp enable command. To disable CDP on the NME-NAM, use the no form of this command.

cdp enable

no cdp enable

* This command is not valid for NAM-1 or NAM-2 devices, the Cisco NAM 2200 Series appliances, or NAM Virtual Blades.

This command has no arguments or keywords.

This command has no default settings.

Command mode

This command is supported only on the NME-NAM-80S and NME-NAM-120S.

This example shows how to enable CDP:

root@localhost.cisco.com# cdp enable

root@localhost.cisco.com#

**classification-mode default**

**To** use default NAM packet classification, use the classification-mode default command. This command is introduced in NAM 6.0(1).

Classification-mode default

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to use default NAM packet classification:

root@nam.localdomain# classification-mode default

Default classification is already in effect

# classification-mode deep-inspect

To use deep packet inspection (EFT feature), use the classification-mode deep-inspect command. This command was introduced in NAM 6.0(1).

Classification-mode deep-inspect

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to use deep packet inspection:

root@nam.localdomain# classification-mode deep-inspect

This operaton will restart NAM services for the changes to take effect.

Do you wish to continue? (y/n) [n]:

clear access log

**cdp interval**

**cdp interval**

**show cdp settings**

# cdp hold-time

To set the Cisco Discovery Protocol (CDP) messages hold time, use the cdp hold-time command. To return the CDP messages hold time to the default value, use the no form of this command.

cdp hold-time time

no cdp hold-time

* This command is not valid for NAM-1 or NAM-2 devices or the Cisco NAM 2200 Series appliances.

|  |  |
| --- | --- |
| time | Specifies the CDP hold time. Range is from 10 to 255 seconds.  |

180 seconds.

Command mode

This example shows how to set the CDP messages hold time:

root@localhost.cisco.com# cdp hold-time 30

root@localhost.cisco.com#

Error! Reference source not found.

# cdp interval

To set the Cisco Discovery Protocol (CDP) messages interval on the NME-NAM, use the cdp interval command. To return the CDP messages interval on the NME-NAM to the default value, use the no form of this command.

cdp interval time

no cdp interval

* This command is not valid for NAM-1 or NAM-2 devices or the Cisco NAM 2200 Series appliances.

|  |  |
| --- | --- |
| time | Specifies the CDP messages interval. Range is from 5 to 254 seconds.  |

60 seconds

Command mode

This example shows how to set the CDP messages interval:

root@localhost.cisco.com# cdp interval 200

root@localhost.cisco.com#

Error! Reference source not found.

# classification-mode default

To use default NAM packet classification, use the classification-mode default command. This command is introduced in NAM 6.0(1).

Classification-mode default

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to use default NAM packet classification:

root@nam.localdomain# classification-mode default

Default classification is already in effect

# classification-mode deep-inspect

To use deep packet inspection (EFT feature), use the classification-mode deep-inspect command. This command was introduced in NAM 6.0(1).

Classification-mode deep-inspect

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to use deep packet inspection:

root@nam.localdomain# classification-mode deep-inspect

This operaton will restart NAM services for the changes to take effect.

Do you wish to continue? (y/n) [n]:

# clear access log

To clear the access log, use the clear access log command.

clear access-log

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to clear the access log:

root@localhost# clear access-log

**secure-clear all**

To clean all users data before shipping, use the secure-clear all command. This was introduced in NAM 6.0(1).

Secure-clear all

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to clean all users data before shipping:

root@nam.localdomain# secure-clear all

This operation will erase completely NAM user data.

(including removing the NAM IP connectivity parameters such

as IP address, To reconfigure the NAM network connectivity,

you must use the switch/router session CLI command or UART port.

Do you wish to continue? (y/n) [n]:

show access-log

# clear captured-data-files

To delete all captured files from the NAM local hard drive, use the clear captured-data-files command.

clear captured-data-files

This command has no default settings.

Command mode

This example shows how to delete all captured files:

root@localhost# clear captured-data-files

# clear counters

To clear counters, use the clear counters command. To date supports only the classification counters. This command was introduced in 6.1(1) release.

clear counters

clear counters classification

This command has no default settings.

Command mode

This example shows how to clear the classification counters:

root@localhost# clear counters classification

# clear monitoring-data

To delete both short term and long term monitoring data, use the clear monitoring-data command. This command will also reset NAM to clean up cached data.

clear monitoring-data

This command has no default settings.

Command mode

This example shows how to clear the access log:

root@localhost# clear monitoring-data

# clear system-alerts

To clear the system alerts, use the clear system-alerts command.

clear system-alerts

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to clear the system alerts:

root@localhost# clear system-alerts

**show system-alerts**

# clear system-passwords

To reset or clear the CLI passwords, use the clear system-passwords command.

clear system-passwords

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to clear the system passwords:

root@localhost# clear system-passwords

# cli idle-timeout

To set an idle/inactivity timeout for the CLI, use the **cli idle-timeout** command. To disable the timeout, use the **no** form of this command. The idle timeout persists across CLI sessions, and is applied to all types of CLI sessions (console, SSH, Telnet). This command was introduced in NAM 6.1(1).

**cli idle-timeout** *timeout*

no cli idle-timeout

|  |  |
| --- | --- |
| *timeout* | Specifies the CLI idle/inactivity timeout. Range is from 10 to 2147483647 seconds. |

The CLI idle timeout is disabled by default.

Command mode

The following example shows how to configure cli timeout settings.

root@nam.localdomain# cli idle-timeout 1800

CLI idle timeout set to 1800 seconds.

root@nam.localdomain# no cli idle-timeout

CLI idle timeout disabled.

root@nam.localdomain#

**Related Commands**

show cli

# clock set

To set the date and time of a Cisco NAM 2000 series appliance, use the clock set command.

clock set <hh:mm:ss:> <mm/dd/yyyy>

* This command is only valid for Cisco NAM 2000 series appliances.

|  |  |
| --- | --- |
| hh:mm:ss: | hh=hour, mm=minutes, ss=seconds |
| mm/dd/yyyy | mm = month, dd=day, yyyy=year |

This command has no default settings.

Command mode

This command is supported only on the Cisco NAM 2200 Series appliances.

The following example shows how to set the clock on the NAM appliance.

root@nam.cisco.com# clock set 06:10:00 08/04/2008

# config clear

To reset the NAM and return it to the factory-default state, use the config clear command.

Please note the behavior of this command has been changed since 6.0(2) release. The network IP parameters will not be reset to factory-default starting from NAM 6.0(2) for config clear without option.

config clear [**all** | **ip**]

|  |  |
| --- | --- |
| all | (Optional) Resets all NAM configurations to factory default including the NAM IP parameters configuration. The NAM reboots automatically for the changes to take effect. |
| ip | (Optional) Resets NAM ip parameters back to factory default. The NAM reboots automatically, and you must session into the NAM from the switch supervisor engine to configure the NAM IP parameters so that the module can come online. |

This command has no default settings.

Command mode

This example shows how to clear the configuration:

root@localhost# config clear

This operation will reset the NAM configurations with the exception

of NAM IP parameters.

This operation will also reboot the NAM to allow the changes to

take effect.

Do you wish to continue? (y/n) [n]:y

Successfully updated the SCCP configuration.

Successfully updated the H.323 configuration.

NAM syslog settings updated successfully.

NAM web interface preferences updated successfully.

Successfully modified the configuration.

NAM will be rebooted now, for the changes to take effect ...

# config network

To import a NAM configuration into the NAM from a specified location or to restore a NAM Virtual Blade license, use the config network command.

config **network** url [config\_filename]

|  |  |
| --- | --- |
| url | Specifies the location of the configuration or license file to upload; ftp://<username>@<host>/<path> |
| config\_filename | Specifies the filename for the configuration file. |

This command has no default settings.

Command mode

This example shows how to download a configuration file to a NAM named kluu-test.config, which is located at the FTP server namlab-pc1 in the user home directory named /home/kluu directory.

root@NAM #

root@NAM # config network ftp://kluu@namlab-pc1//home/kluu/kluu-test.config

Downloading ftp://kluu@namlab-pc1//home/kluu/kluu-test.config, please wait ...

Password for kluu@namlab-pc1:

ftp://kluu@namlab-pc1//home/kluu/kluu-test.config (9K)

/tmp/lrcfile.txt.1007 [########################] 9K | 4916.90K/s

9748 bytes transferred in 0.00 sec (4274.44k/sec)

Download completed.

Configuring the NAM. This may take few minutes, please wait ...

NAM configuration completed.

To view the results, use the command 'show log config'.

root@NAM #

**configupload**

# config upload

To upload the running NAM configuration to a specified location, use the config upload command.

config **upload** url [config\_filename]

|  |  |
| --- | --- |
| url | Specifies the location of the configuration or license file to upload; ftp://<username>@<host>/<path> |
| config\_filename | Specifies the filename for the configuration file. |

This command has no default settings.

Command mode

If config\_filename is not specified when this command is issued, NAM will assign a default config file name.

This example shows how to upload the NAM running configuration to the FTP server named namlab-pc1 with a filename of example.config:

root@NAM# config upload ftp://kluu@namlab-pc1.cisco.com example.config

Building configuration, please wait... Done.

Uploading the configuration to 'example.config'

on 'ftp://kluu@namlab-pc1.cisco.com', This may take few minutes ...

Password:

Successfully uploaded the NAM configuration.

root@NAM#

**config network**

# coredump

To retrieve the core dump file, use the coredump command.

coredump ftp://user:passwd@host/full-path/

|  |  |
| --- | --- |
| ftp://user:passwd@host/full-path/ | Sets the path to the core dump file. |

This command has no default settings.

Command mode

This example shows how to retrieve a core dump:

root@localhost# coredump ftp://user:passwd@host/full-path/

# data-source erspan

To create ERSPAN (Encapsulated Remote SPAN) data-source, use the data-source erspan command.

**data-source erspan**

This command has no default settings.

Command mode

When you enter the data-source erspan submode, the following commands are available:

* device-id—ERSPAN device ID. This is a mandatory value.
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the exit command section.
* **help**—Displays help and keeps you in the application group subcommand mode; see the “help” command section.
* name string—Sets the data-source erspan name. This is a mandatory value.
* session-id—ERSPAN session ID
* show—Shows the current configuration which is applied on exit

This example shows how to create an ERSPAN data-source:

root@nam235Cat6k.cisco.com# data-source erspan

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-data-source-erspan)# ?

? - display help

cancel - discard changes and exit from subcommand mode

device-id - ERSPAN device ID (\*)

exit - create data-source and exit from sub-command mode

help - display help

name - data-source name (\*)

session-id - ERSPAN session ID

show - show current config that will be applied on exit

(\*) - denotes a mandatory field for this configuration.

# data-source netflow

To create NetFlow Data Export (NDE) data-source, use the data-source netflow command.

**data-source netflow**

This command has no default settings.

Command mode

When you enter the data-source netFlow submode, the following commands are available:

* device-id—NetFlow device ID. This is a mandatory value.
* engine-id—NetFlow engine ID
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode.
* **help**—Displays help and keeps you in the application group subcommand mode.
* name string—Sets the netFlow data-source name. This is a mandatory value.
* show—Shows the current configuration which is applied on exit

This example shows how to create a netFlow data-source:

root@nam235Cat6k.cisco.com# data-source netflow

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-data-source-netflow)# ?

? - display help

cancel - discard changes and exit from subcommand mode

device-id - netflow device ID (\*)

engine-id - netflow Engine ID

exit - create data-source and exit from sub-command mode

help - display help

name - data-source name (\*)

show - show current config that will be applied on exit

(\*) - denotes a mandatory field for this configuration.

# data-source pa

To create performance agent (pa) data-source, use the data-source pa command.

**data-source pa**

This command has no default settings.

Command mode

This command is supported on all NAM platforms.

When you enter the data-source netFlow submode, the following commands are available:

* device-id—NetFlow device ID. This is a mandatory value.
* engine-id—NetFlow engine ID
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode.
* **help**—Displays help and keeps you in the application group subcommand mode.
* name string—Sets the netFlow data-source name. This is a mandatory value.
* show—Shows the current configuration which is applied on exit

This example shows how to create a pa data-source:

root@nam235Cat6k.cisco.com# data-source pa

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-data-source-netflow)# ?

? - display help

cancel - discard changes and exit from subcommand mode

device-id - netflow device ID (\*)

engine-id - netflow Engine ID

exit - create data-source and exit from sub-command mode

help - display help

name - data-source name (\*)

show - show current config that will be applied on exit

(\*) - denotes a mandatory field for this configuration.

# data-source waas

To create Wide Area Application Services (WAAS) data-source, use the data-source waas command.

**data-source waas**

This command has no default settings.

Command mode

When you enter the data-source waas submode, the following commands are available:

* device-id—WAAS device ID. This is a mandatory value.
* segment—This is the network segment that needs to be added to the data-source. This is a mandatory value.
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** section.
* **help**—Displays help and keeps you in the application group subcommand mode; see the **help** command section.
* name string—Sets the waas data-source name. This is a mandatory value.
* show—Shows the current configuration which is applied on exit.

This example shows how to create a WAAS data-source:

root@nam235Cat6k.cisco.com# data-source waas

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-data-source-waas)# ?

? - display help

cancel - discard changes and exit from subcommand mode

device-id - WAAS device ID (\*)

exit - create data-source and exit from sub-command mode

help - display help

name - data-source name (\*)

segment - network segment to be added to data-source (\*)

show - show current config that will be applied on exit

(\*) - denotes a mandatory field for this configuration.

# debug log disable

To disable debug logging, use the debug log disable command.

debug log disable

This command has no arguments or keywords.

This command has no default behavior or settings.

Command mode

The following example disables all debug logging:

root@nam.cisco.com# debug log disable

# debug log enable

To enable debug logging, use the debug log enable command.

debug log enable

This command has no arguments or keywords.

This command has no default behavior or settings.

Command mode

The following example enables all debug logging:

root@nam.cisco.com# debug log enable

# debug log level

To set the debug log level for each module running in NAM system, use the debug log-level command.

show debug log level <log-feature> <log-level>

|  |  |
| --- | --- |
| log-feature | Possible feature names include the following: ART, CAPTURE, COLL\_SHARED, DSMON\_HOST, DSMON\_MATRIX, DSMON\_PDIST, DSMON\_STATS, ENTITY, ETHERSTATS, FM, FR, MAIN, MISC, RMON, RPC, DSRC, PARSER, PPROC, RTP, METRIC\_ENGINE, OTHER, PORT\_TABLE, MPLS\_STATS, POLLD, RMON1\_HOST, RMON1\_MATRIX, RMON2\_ADDRMAP, RMON2\_HOST, RMON2\_MATRIX, RMON2\_PDIST, SMON\_PRIO, SMON\_VLAN, SNMP, SRSNMP, SWPOLLD, TREND\_DAEMON, TREND\_RPC, TREND\_SNMP, URL\_COLLECTION, WAAS, |
| log-level | A value between 0 and 7 which represents the following log levels:0—Critical1—Error2—Warning3—Notice4—Info5—Debug6—Debug27—Debug3 |

This command has no default behavior or settings.

Command mode

The following example shows how to set the automated response time (ART) feature to display all log messages up to log level 2. This command will log all messages generated by the ART module that have log levels set to critical, error, and warning.

root@nam.cisco.com# debug log level ART 2

# debug log metric-engine

To set debug log metric-engine, use the **debug log metric-engine** command.

debug log metric-engine

This command has no arguments or keywords.

No default behavior or values.

Command mode

The following example sets the debug log level metric-engine:

root@nam.cisco.com# debug log metric-engine

# debug log reset

To reset debug logging level back to default settings, use the debug log reset command.

debug log reset

This command has no arguments or keywords.

No default behavior or values.

Command mode

The following example resets all debug log levels back to default values:

root@nam.cisco.com# debug log reset

# device erspan

To create an ERSPAN (Encapsulated Remote SPAN) device, use the device erspan command.

**device erspan**

This command has no default settings.

Command mode

When you enter the device erspan submode, the following commands are available:

* address—IP address of the device. This is a mandatory value.
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command section.
* **help**—Displays help and keeps you in the application group subcommand mode; see the **help** command section.
* show—Shows the current configuration which is applied on exit

This example shows how to create an ERSPAN device:

root@nam235Cat6k.cisco.com# device erspan

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-device-erspan)# ?

? - display help

address - device IP address (\*)

cancel - discard changes and exit from subcommand mode

exit - create device and exit from sub-command mode

help - display help

show - show current config that will be applied on exit

(\*) - denotes a mandatory field for this configuration.

# device netflow

To create a NetFlow Data Export (NDE) device, use the device netflow command.

**device netflow**

This command has no default settings.

Command mode

When you enter the device netFlow submode, the following commands are available:

* address—IP address of the device. This is a mandatory value.
* community—SNMPv2c community string
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command section.
* **help**—Displays help and keeps you in the application group subcommand mode; see the **help** command section.
* show—Shows the current configuration which is applied on exit.
* snmp-version—The version of SNMP that is used to communicate with the device
* v3-auth-passphrase—SNMPv3 authentication passphrase
* v3-auth-protocol—SNMPv3 authentication protocol
* v3-priv-passphrase—SNMPv3 privacy passphrase
* v3-priv-protocol—SNMPv3 privacy protocol
* v3-sec-level—SNMPv3 security level
* v3-username—SNMPv3 username

This example shows how to create a netFlow device:

root@nam235Cat6k.cisco.com# device netflow

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-device-netflow)# ?

? - display help

address - device IP address (\*)

cancel - discard changes and exit from subcommand mode

community - SNMPv2c community string

exit - create device and exit from sub-command mode

help - display help

show - show current config that will be applied on exit

snmp-version - SNMP version to use to communicate with device

v3-auth-passphrase - SNMPv3 authentication passphrase

v3-auth-protocol - SNMPv3 authentication protocol

v3-priv-passphrase - SNMPv3 privacy passphrase

v3-priv-protocol - SNMPv3 privacy protocol

v3-sec-level - SNMPv3 security level

v3-username - SNMPv3 username

(\*) - denotes a mandatory field for this configuration.

# device waas

To create Wide Area Application Services (WAAS) device, use the device waas command.

**device waas**

This command has no default settings.

Command mode

When you enter the device WAAS submode, the following commands are available:

* address—IP address of the device. This is a mandatory value.
* passthru—This is the passthru enable or disable traffic from the WAAS device.
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the exit command section.
* **help**—Displays help and keeps you in the application group subcommand mode; see the “help” command section.
* show—Shows the current configuration which is applied on exit.

This example shows how to create a WAAS device:

root@nam235Cat6k.cisco.com# **device waas**

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam235Cat6k.cisco.com(sub-device-waas)# ?

? - display help

address - device IP address (\*)

cancel - discard changes and exit from subcommand mode

exit - create device and exit from sub-command mode

help - display help

passthru - enable/disable passthru traffic from WAAS device

show - show current config that will be applied on exit

(\*) - denotes a mandatory field for this configuration.

# 3: NAM CLI Commands: email – managed-device community\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter provides information about the following commands:

* email
* entity alias
* entity assetid
* exsession
* exit
* help
* ip address
* ip broadcast
* ip domain
* ip gateway
* ip host
* ip hosts add
* ip hosts delete
* ip http port
* ip http secure generate
* ip http secure install certificate
* ip http secure port
* ip http secure server
* ip http server
* ip http tacacs+
* ip interface
* ip nameserver
* license install
* logout
* managed-device address
* managed-device community

# email

To set up an e-mail server that sends both alarm and report data through e-mail, enable or disable alarm messages sent through e-mail, and to enter the subcommand mode, use the email command. To remove the e-mail server, use the no email server command. To stop sending out both scheduled report data and alarm messages through e-mail, use the no email alarm command.

email

no email server

**no email alarm**

This command has no arguments or keywords.

This command has no default settings.

Command mode

*
* Recipients are the alarm message recipients. Report data recipients are not supported on CLI.

When you enter the e-mail subcommand mode, the following commands are available:

* **?** or **help**—Displays help; see the “**Error! Reference source not found.**” command section.
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the exit command section.
* server email-server—Specifies the e-mail server name.
* advanced enable – Enables advanced email settings (as of NAM 6.1(1))
* advanced disable – Disables advanced email settings (as of NAM 6.1(1))
* **alarm enable**— Enables sending alarm messages through e-mail.
* **alarm disable**—Disables sending alarm messages through e-mail.
* **alarm recipients** space-separated-list-of-email-addresses— List of email addresses like admin@domain.com, user@domain.com.
* **encryption SSL** – Enable email encryption using SSL (as of NAM 6.1(1))
* **encryption TLS –** Enable email encryption using TLS
* **port –** set email server port

This example shows how to set up the NAM to send scheduled reports through e-mail to abc@example.com and xyz@example.com:

root@localhost# email

proot@localhost(sub-email)# server example-email.domain.com

root@localhost(sub-email)# alarm enable

root@localhost(sub-email)# alarm recipients admin@domain.com another\_admin@domain.com

root@localhost(sub-email)# exit

Successfully set email configuration settings.

**show debug metric-engine**

# entity alias

To configure an entity alias for the entity MIB, use the entity alias command.

entity alias string

|  |  |
| --- | --- |
| String | Specifies the entity string used to configure the entPHysicalAlias. |

This command has no default settings.

Command mode

The entity MIB makes the entPhysicalTable and entLastChangeTime available through SNMP.

The clear configuration command deletes the entity alias and asset ID by setting them to an empty string.

This example shows how to log out of the NAM:

root@localhost# entity alias 123456

**show entity**

# entity assetid

To configure an entity MIB asset ID, use the entity assetid command.

entity assetid string

|  |  |
| --- | --- |
| String | Specifies the entity string used to configure the entPHysicalAssetID. |

This command has no default settings.

Command mode

The entity MIB makes the entPhysicalTable and entLastChangeTime available through SNMP.

The clear configuration command deletes the entity alias and asset ID by setting them to an empty string.

This example shows how to log out of the NAM:

root@localhost# entity assetid 1234566

**show entity**

# exit

To log out of the system or to leave a subcommand mode, use the **exit** command.

exit

This command has no arguments or keywords.

This command has no default settings.

Command mode

To leave a subcommand mode, use the **exit** command. The **exit** command saves any changes before leaving the submode.

This example shows how to log out of the NAM:

root@localhost# exit

# exsession

To enable or disable outside logins, use the exsession command.

exsession **on** [**ssh**]

exsession off

|  |  |
| --- | --- |
| **on** | Enables outside logins. |
| **off** | Disables outside logins. |
| **ssh** | (Optional) Sets the outside logins to SSH. |

This command has no default settings.

Command mode

A strong crypto patch is required if you use the ssh option.

This example shows how to allow outside logins to the NAM:

root@localhost# exsession on

# flow-table

To enable or disable extended keys in the flow table. Only tos keys are supported to date. This command was introduced in 6.1(1) release.

flow-table

flow-table extended-key tos enable|disable

This command has no default settings.

Command mode

Example:

flow-table extended-key tos enable

# ftp

To set the FTP server and directory for storing scheduled reports, use the ftp command. To disable FTP scheduled reports, use the no form of this command.

ftp

no ftp

This command has no arguments or keywords.

This command has no default settings.

Command mode

When you enter the FTP subcommand mode, the following commands are available:

* **?** or **help**—Displays help; see the **help** command section.
* **cancel**—Discards changes and exits from the subcommand mode.
* **directory** WORD—Specifies the FTP location on the FTP server.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit**  command.
* password WORD—Specifies the user password on the FTP server.
* **index**—A unique integer identifying the FTP entry
* user WORD—Specifies the user name on the FTP server.
* **server** WORD—Specifies the FTP server name or IP address.

This example shows how to set the FTP server for storing scheduled reports:

root@localhost# ftp

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@localhost(sub-ftp)# ?

? - display help

cancel - discard changes and exit from subcommand mode

directory - FTP location at the FTP server

exit - exit from subcommand mode

help - display help

index - a unique integer identifying the ftp entry

password - password of the user at the FTP server

server - set FTP server

user - user name at the FTP server

# help

To display help, use the help command or ?. You must press the Enter key after entering the ?.

help | ?

This command has no arguments or keywords.

This command has no default settings.

Command mode or subcommand mode.

This example shows how to display help:

nam.domain.com# help

? - display help

application - configure an application [group]

audit-trail - enable logging Web GUI and CLI accesses

autocreate-data-source - enable data source autocreation feature

clear - clear access log / system alerts

# ip address

To set the system IP address, use the ip address command. IPv6 support was introduced in NAM 6.0(1).

ip **address** ip-address subnet-mask

|  |  |
| --- | --- |
| ip-address  | Sets the system IP address. |
| subnet-mask | Sets the subnet mask. |

This command has no default settings.

Command mode

After setting the IP address, the gateway address may be set to 0.0.0.0. When this situation occurs, use the ip gateway command to set the gateway address.

The broadcast address is automatically set with an address that is created using the new IP address and network mask. To select a different broadcast address, use the ip broadcast command.

This example shows how to set the system IP address:

root@localhost# ip address 172.20.104.74 255.255.255.192

IP address and netmask configured successfully.

NOTE: Default gateway address has been reset to 0.0.0.0

Please use 'ip gateway' command to configure it.

root@localhost# ip gateway 172.20.104.66

root@localhost# show ip

IP address: 172.20.104.74

Subnet mask: 255.255.255.192

IP Broadcast: 172.20.255.255

DNS Name: namlab-kom8.cisco.com

Default Gateway: 172.20.104.66

Nameserver(s): 171.69.2.133

HTTP server: Enabled

HTTP secure server: Disabled

HTTP port: 80

HTTP secure port: 443

TACACS+ configured: No

Telnet: Enabled

SSH: Disabled

root@localhost#

**ip broadcast**

**ip domain**

**ip host**

# ip broadcast

To set the system broadcast address, use the ip broadcast command.

ip **broadcast** broadcast-address

|  |  |
| --- | --- |
| broadcast-address  | Sets the system broadcast address. |

This command has no default settings.

Command mode

This example shows how to set the system broadcast address:

root@localhost# ip broadcast 172.20.104.127

root@localhost#

**ip broadcast**

**ip domain**

**ip host**

**show ip**

# ip domain

To set the system domain name, use the ip domain command.

ip **domain** name

|  |  |
| --- | --- |
| Name | Sets the system domain name. |

This command has no default settings.

Command mode

This example shows how to set the IP domain name:

root@nam# **ip domain** **cisco.com**

root@nam.cisco.com#

**ip broadcast**

**ip domain**

**ip host**

**show ip**

# ip gateway

To set the system default gateway address, use the ip gateway command.

ip **gateway** default-gateway

|  |  |
| --- | --- |
| default-gateway | Sets the default gateway address. |

This command has no default settings.

Command mode

This example shows how to set the IP gateway address:

root@localhost# ip gateway 123.34.56.0

**ip broadcast**

**ip domain**

**ip host**

**show ip**

# ip host

To set the system hostname, use the ip host command.

ip **host** name

|  |  |
| --- | --- |
| Name | Sets the IP hostname. |

This command has no default settings.

Command mode

This example shows how to set the IP hostname:

root@NAM.cisco.com# ip host orion

root@orion.cisco.com#

**ip broadcast**

**ip domain**

**show ip**

# ip hosts add

To add or replace host entries, use the ip hosts add command.

ip **hosts add** ip-address host-name [**alias1**] [**alias2**]

ip hosts add ftp://user:passwd@host/full-path/filename

|  |  |
| --- | --- |
| ip-address | Sets the host IP address. |
| host-name | Sets the hostname which can be a FTP URL with a filename. |
| alias1 alias2 | (Optional) Sets the host alias. |
| ftp://user:passwd@host/full-path/filename | Sets the path to the host parameters file location. |

This command has no default settings.

Command mode

Use the ip hosts add ftp://user:passwd@host/full-path/filename command to import host entries to the NAM. A maximum of 1,000 entries can exist on the NAM.

This example shows how to add a specific IP host:

root@localhost# ip hosts add 30.50.68.10 orion

**ip hosts delete**

**show hosts**

# ip hosts delete

To delete host entries, use the ip hosts delete command.

ip **hosts delete** ip-address

ip hosts delete ftp://user:passwd@host/full-path/filename

|  |  |
| --- | --- |
| ip-address | Sets the host IP address. |
| ftp://user:passwd@host/full-path/filename | Sets the path to the host parameters file location. |

This command has no default settings.

Command mode

This example shows how to delete a specific IP host:

root@localhost# ip hosts delete 30.50.68.10 orion

**ip hosts add**

# ip http port

To set the HTTP port, use the ip http port command.

ip http port 1-65535

|  |  |
| --- | --- |
| 1-65535 | Specifies a port number in the range of 1 through 65535. |

Not all ports are available to be assigned. Most browsers block ports that are used for other applications. Commonly-Blocked Ports lists the commonly blocked ports.

|  |
| --- |
| * Commonly-Blocked Ports
 |
| Port  | Application |  | Port | Application |  | Port  | Application |  | Port | Application |
| 1 | tcpmux  |  | 43 | nicname  |  | 117 | uucp-path  |  | 531 | chat |
| 7 | echo  | 53 | domain  | 119 | NNTP  | 532 | netnews |
| 9 | discard  | 77 | priv-rjs  | 123 | NTP  | 540 | uucp |
| 11 | systat  | 79 | finger  | 135 | loc-srv / epmap  | 556 | remotefs |
| 13 | daytime  | 87 | ttylink  | 139 | netbios  | 563 | NNTP+SSL  |
| 15 | netstat  | 95 | supdup  | 143 | IMAP2  | 587 | submission  |
| 17 | qotd  | 101 | hostriame  | 179 | LDAP  | 601 | syslog  |
| 19 | chargen  | 102 | iso-tsap  | 389 | LDAP  | 636 | LDAP+SSL  |
| 20 | ftp data  | 103 | gppitnp  | 465 | SMTP+SSL  | 993 | IMAP+SSL  |
| 21 | ftp control  | 104 | acr-nema  | 512 | print / exec  | 995 | POP3+SSL  |
| 22 | ssh  | 109 | POP2  | 513 | login | 4045 | lockd |
| 23 | telnet  | 110 | POP3  | 514 | shell | 6000 | X11 |
| 25 | smtp  | 111 | sunrpc  | 515 | printer |  |  |
| 37 | time  | 113 | auth  | 526 | tempo |  |  |
| 42 | name  | 115 | sftp  | 530 | courier |  |  |

This command has no default settings.

Command mode

This example shows how to specify an HTTP port for the NAM:

root@localhost# ip http port 233

**ip http secure generate**

**ip http server**

**ip http tacacs+**

**show ip**

# ip http secure generate

To generate a certificate request, use the ip http secure generate command.

ip http secure generate {**certificate-request** | **self-signed-certificate**}

|  |  |
| --- | --- |
| certificate-request  | Generates a certificate request. |
| self-signed-certificate | Generates a self-signed certificate. |

This command has no default settings.

Command mode

This example shows how to set up a secure server:

root@localhost# ip http secure generate certificate-request

**ip http port**Error! Reference source not found.

# ip http secure install certificate

To install a certificate, use the ip http secure install certificate command.

**ip http secure install certificate**

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to set up a secure server:

root@localhost# ip http secure install certificate

**ip**

# ip http secure port

To set up a secure server port, use the ip http secure port command.

ip http secure port port

|  |  |
| --- | --- |
| Port | Sets the HTTP secure port.  |

Not all ports are available to be assigned. Most browsers block ports that are used for other applications. Commonly-Blocked Ports on page 92 lists the commonly blocked ports.

This command has no default settings.

Command mode

This example shows how to set up a secure server port:

root@localhost# ip http secure port 30

**ip**

# ip http secure server

To set up a secure server, use the ip http secure server command.

ip http secure server {**enable** | **disable**}

|  |  |
| --- | --- |
| **server** enable | disable | Enables or disables the HTTP server. |

This command has no default settings.

Command mode

*

A strong crypto patch is required before applying this command.

This example shows how to set up a secure server:

root@localhost# ip http secure server enable

**ip**

# ip http server

To enable a HTTP server, use the ip http server command.

ip http server {enable | disable}

|  |  |
| --- | --- |
| **enable** | Enables the HTTP server. |
| **disable** | Disables the HTTP server. |

This command has no default settings.

Command mode

This example shows how to enable a HTTP server:

root@localhost# ip http server enable

**ip**

# ip http tacacs+

To enable a TACACS+ server, use the ip http tacacs+ command.

ip http tacacs+ enable primary-srv [**backup-srv**] [**en-secret-key** encrypted-secret-key]

ip http tacacs+ **disable**

|  |  |
| --- | --- |
| **disable** | Disables the TACACS+ server. |
| **enable** | Enables the TACACS+ server. |
| primary-srv | Specifies the primary TACAC+ server. |
| backup-srv | (Optional) Specifies the backup TACACS+ server. |
| en-secret-key | (Optional) Argument name to enable the secret key. |
| encrypted-secret-key | (Optional) Argument value. |

This command has no default settings.

Command mode

The en-secret-key keyword is used only during the importing of NAM configurations. This key cannot be used unless you can specify a DES-encrypted string as the argument to this keyword, as in this example:

root@localhost# ip http tacacs+ enable 10.0.0.1 10.0.0.2 en-secret-key "dEAF="

These examples show how to enable and disable TACACS+.

To enable TACACS+, enter this command:

root@hostname.cisco.com# ip http tacacs+ enable 10.0.0.1 10.0.0.2

Secret key:

Repeat secret key:

Successfully enabled Tacacs+

root@hostname.cisco.com# show ip

IP address: 172.20.98.177

Subnet mask: 255.255.255.192

IP Broadcast: 172.20.255.255

DNS Name: hostname.cisco.com

Default Gateway: 172.20.98.129

Nameserver(s): 171.69.2.133

HTTP server: Enabled

HTTP secure server: Disabled

HTTP port: 80

HTTP secure port: 443

TACACS+ configured: Yes

TACACS+ primary server: 10.0.0.1

TACACS+ backup server : 10.0.0.2

Telnet: Enabled

SSH: Disabled

root@hostname.cisco.com#

To disable TACACS+, enter this command:

root@hostname.cisco.com# ip http tacacs+ disable

TACACS+ disabled successfully.

root@hostname.cisco.com# show ip

IP address: 172.20.98.177

Subnet mask: 255.255.255.192

IP Broadcast: 172.20.255.255

DNS Name: hostname.cisco.com

Default Gateway: 172.20.98.129

Nameserver(s): 171.69.2.133

HTTP server: Enabled

HTTP secure server: Disabled

HTTP port: 80

HTTP secure port: 443

TACACS+ configured: No

Telnet: Enabled

SSH: Disabled

root@hostname.cisco.com#

**ip**

# ip interface

To select the external port or the internal ports for the NME-NAM, use the ip interface command.

ip interface external | internal

* This command is not valid for NAM-1 or NAM-2 devices, the Cisco NAM 2200 Series appliances, or the Cisco NAM Virtual Blades.

|  |  |
| --- | --- |
| **external** | Selects the RJ-45 Fast Ethernet connector on the NME-NAM. |
| **internal** | Selects the internal LAN segment to the router through the PCI interface for IP communication (for example Telnet, SNMP, HTTP, and so forth) to the NME-NAM. |

This command has no default settings.

Command mode

This command is supported only on the NME-NAM.

This example shows how to specify an interface port for the NME-NAM:

root@localhost# ip interface external

**ip**
**show ip**

# ip nameserver

To set or disable system name server entries, use the ip nameserver command.

ip nameserver ip-addr ip-addr ip-addr

or

ip nameserver disable

|  |  |
| --- | --- |
| ip-addr | Sets the name server address. |
| **disable** | Disables the name server entries. |

This command has no default settings.

Command mode

This example shows how to set a system name server:

root@localhost# ip nameserver 171.69.2.133

**ip**
**show ip**

# license install

To install a license file on a WAE device that has installed NAM Virtual Blade software, use the license install command.

license install url

|  |  |
| --- | --- |
| url | Specifies the location of the license file to install; ftp://<username>@<host>/<path>/<license\_filename> |

This command has no arguments or keywords.

This command has no default settings.

Command mode

This command is valid only on NAM WAAS Virtual Blade platform.

This example shows how to install the license file on the WAE device that has NAM installed on it:

root@localhost# license install ftp://joseph@host\_name/usr/

# logout

To log out of the system, use the logout command.

logout

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to log out of the NAM:

root@localhost# logout

# managed-device address

To configure the managed device address, use the managed-device address command. To remove the managed device ip address, use the no managed-device address. This no manage-device command was introduced in NAM 6.0(1).

no managed-device address

managed-device address  <ip-address>

* This command is not supported on NAM-1, NAM-2, NME-NAM-80S, NME-NAM-120S and the NAM Virtual Blade devices.

|  |  |
| --- | --- |
| ip-address  | Specifies the IP address of the managed device. |

No default behavior or values.

Command mode

This command is supported only on Cisco NAM 2200 Series appliances.

The following example sets the managed device IP address, and then shows the managed device:

root@nam.cisco.com# managed-device address 10.0.0.1

root@nam.cisco.com# show managed-device

root@nam.cisco.com# 10.0.0.1

root@nam.localdomain# no managed-device address

Managed Device Address removed if any!

root@nam.localdomain#

# managed-device community

To configure the managed device SNMP community, use the managed-device community command. To remove the managed device community string, use the no managed-device community command. This remove command was introduced in NAM 6.0(1).

No managed-device community

managed-device community <rw-community>

* This command is not supported on NAM-1, NAM-2, NME-NAM-80S, NME-NAM-120S and the NAM Virtual Blade devices.

|  |  |
| --- | --- |
| rw-community | Specifies the SNMP community for read/write operations. |

None.

Command mode

This command is supported only on Cisco NAM 2200 Series appliances.

The following example sets the managed-device community:

root@nam.cisco.com# managed-device community

root@nam.cisco.com#

root@nam.localdomain# no managed-device community

Managed Device Community string removed if any!

root@nam.localdomain#

# 4: NAM CLI Commands: metric export host - show certificate request\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter describes the following NAM CLI commands:

* metric export host
* metric export non-waas traffic
* monitor data-aggr-intv

To set data aggregation intervals, use the monitor data-aggr-intv command. This command was introduced in NAM 6.0(1).

**Monitor data-aggr-intv**

This command has no default settings.

Command mode

When you enter the monitor data-aggr-intv submode, the following commands are available:

* **?**—Displays help. (Introduced in 6.0(2)
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—exits from the subcommand mode.
* **help**—Displays help.
* hosts-user-defined enable—enable user-defined hosts.
* hosts-user-defined disable—disable user-defined hosts.
* intf-stats-polling— enable or disable managed device interface stats polling. (Introduced in 6.0(2))
* long-term-intf [min]—Specify long term interval for managed device interface stats (min).
* **long-term-rsp-time [min]**—Specify long term interval for application response time (min).
* long-term-traffic [min]—Specify long term interval for traffic (min).
* short-term-intf [min]—Specify short term interval for managed device interface stats (min).
* **short-term-rsp-time [min]**—Specify short term interval for application response time (min).
* short-term-traffic [min]—Specify short term interval for traffic/media (min).

This example shows how to set data aggregation intervals:

root@nam.localdomain# monitor data-aggr-intv

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam.localdomain(sub-data-aggr-intv)

# root@nam.localdomain(sub-data-aggr-intv)# ?

? - display help

cancel - discard changes and exit from subcommand mode

exit - exit from the subcommand mode

help - display help

hosts-user-defined - collect only hosts from user-defined sites

long-term-intf - specify long term interval for managed device interface stats (min)

long-term-rsp-time - specify long term interval for application response time (min)

long-term-traffic - specify long term interval for traffic (min)

short-term-intf - specify short term interval for managed device interface stats (min)

short-term-rsp-time - specify short term interval for application response time (min)

short-term-traffic - specify short term interval for traffic/media (min)

root@nam.localdomain(sub-data-aggr-intv)#

* monitor nbar
* monitor protocol encapsulation
* monitor rtp-stream enable
* monitor rtp-stream filter
* monitor rtp-stream threshold
* monitor urlcollection
* monitor urlfilter
* netflow input port
* nslookup
* password
* password strong-policy
* [patch](#_Toc330562001)
* [pid-sn](#_Toc330562002)
* [ping](#_Toc330562003)
* [preferences](#_Toc330562004)
* [protocol esp-null-heuristic](#_Toc330562005)
* [reboot](#_Toc330562006)
* [reboot -helper](#_Toc330562007)
* [reboot -golden](#_Toc330562008)
* [remote-storage](#_Toc330562009)
* [remote-storage fcoe](#_Toc330562010)
* [remote-storage iscsi](#_Toc330562011)
* [remote-storage sas](#_Toc330562012)
* [rmwebusers](#_Toc330562013)
* [show access-log](#_Toc330562014)
* [show application app-id](#_Toc330562015)
* [show application eng-id](#_Toc330562016)
* [show application group](#_Toc330562017)
* [show audit-trail](#_Toc330562018)
* [show autocreate-data-source](#_Toc330562019)
* [show cdb](#_Toc330562020)
* [show cdp settings](#_Toc330562021)
* [show certificate](#_Toc330562022)

# metric export host

To configure the metric export host, use the metric export host command. To disable metric export, use the no form of this command.

metric export host ip-address [port]

no metric export

|  |  |
| --- | --- |
| ip-address | Specifies the IPv4 address of the external reporting console.  |
| port | Port the external reporting console is listening on for incoming packets (optional). |

The default port is 9995.

Command mode

Use this command to export ART metrics to an external reporting console.

The following example specifies the reporting console’s IP address as the source to collect ART metrics, then removes this configuration.

root@nam.cisco.com# metric export 10.0.0.1 9995

root@nam.cisco.com# no metric export

# metric export non-waas traffic

To send SPAN traffic (non-WAAS traffic) to an external reporting console, use the metric export non-waas traffic command. To disable metric export, use the no form of this command.

metric export non-waas traffic

no metric export non-waas traffic

This command has no arguments or keywords.

Export is disabled.

Command mode

Use this command to export non-waas (SPAN traffic) metrics to an external reporting console.

The following example shows how to send non-WAAS traffic to an external reporting console, then removes this configuration:

root@nam.cisco.com# metric export non-waas traffic

root@nam.cisco.com# no metric export non-waas traffic

# monitor data-aggr-intv

To set data aggregation intervals, use the monitor data-aggr-intv command. This command was introduced in NAM 6.0(1).

**Monitor data-aggr-intv**

This command has no default settings.

Command mode

When you enter the monitor data-aggr-intv submode, the following commands are available:

* **?**—Displays help. (Introduced in 6.0(2)
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—exits from the subcommand mode.
* **help**—Displays help.
* hosts-user-defined enable—enable user-defined hosts.
* hosts-user-defined disable—disable user-defined hosts.
* intf-stats-polling— enable or disable managed device interface stats polling. (Introduced in 6.0(2))
* long-term-intf [min]—Specify long term interval for managed device interface stats (min).
* **long-term-rsp-time [min]**—Specify long term interval for application response time (min).
* long-term-traffic [min]—Specify long term interval for traffic (min).
* short-term-intf [min]—Specify short term interval for managed device interface stats (min).
* **short-term-rsp-time [min]**—Specify short term interval for application response time (min).
* short-term-traffic [min]—Specify short term interval for traffic/media (min).

This example shows how to set data aggregation intervals:

root@nam.localdomain# monitor data-aggr-intv

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam.localdomain(sub-data-aggr-intv)

# root@nam.localdomain(sub-data-aggr-intv)# ?

? - display help

cancel - discard changes and exit from subcommand mode

exit - exit from the subcommand mode

help - display help

hosts-user-defined - collect only hosts from user-defined sites

long-term-intf - specify long term interval for managed device interface stats (min)

long-term-rsp-time - specify long term interval for application response time (min)

long-term-traffic - specify long term interval for traffic (min)

short-term-intf - specify short term interval for managed device interface stats (min)

short-term-rsp-time - specify short term interval for application response time (min)

short-term-traffic - specify short term interval for traffic/media (min)

root@nam.localdomain(sub-data-aggr-intv)#

# monitor nbar

To enable supervisor NBAR statistics polling, use the monitor nbar command. To disable polling, use the no form of this command. This command has been removed in 6.1(1) release.

monitor nbar

no monitor nbar

This command has no arguments or keywords.

This command has no defaults.

Command mode

The NBAR-PD-MIB must be present to enable the collection of statistical information. The NAM-3 statistics are polled from the supervisor engine.

This example shows how to enable NBAR statistics polling:

root@localhost.cisco.com# monitor nbar

Successful enable nbar collection.

root@localhost.cisco.com# no monitor nbar

Successfully disable nbar collection.

This example shows how to display NBAR statistics polling:

root@localhost.cisco.com# show monitor nbar

nbar collection enabled

# monitor protocol encapsulation

To set the protocol encapsulation, use the **monitor protocol encapsulation** command.To disable the protocol encapsulation, use the no form of this command. This command is removed in NAM 6.0(1).

monitor protocol encapsulation

no monitor protocol encapsulation

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to set the monitor protocol encapsulation.

root@nam.cisco.com# monitor protocol encapsulation

gre-ip - encapsulation type

gtp - encapsulation type

ip-esp - encapsulation type

ip-ipv4 - encapsulation type

ip-ipv6 - encapsulation type

root@nam.cisco.com# monitor protocol encapsulation

**show monitor protocol encapsulation**

# monitor rtp-stream enable

To enable RTP stream monitoring, use the monitor rtp-stream enable command. To disable RTP stream monitoring, use the no form of this command.

monitor rtp-stream enable

no monitor rtp-stream enable

This command has no default settings.

Command mode

This example shows how to enable RTP stream monitoring.

root@localhost# monitor rtp-stream enable

This example shows how to disable RTP stream monitoring.

root@localhost# no monitor rtp-stream enable

**monitor rtp-stream filter**

# monitor rtp-stream filter

To set a RTP stream filtering entry, use the monitor rtp-stream filter command. To remove a RTP stream filtering entry, use the no form of this command.

monitor rtp-stream filter source-address source-mask dest-address dest-mask

|  |  |
| --- | --- |
| source-address | Specifies the source address of the RTP stream being filtered. |
| source-mask | Specifies the subnet mask of the source address of the RTP stream being filtered. |
| dest-address | Specifies the destination address of the RTP stream being filtered. |
| dest-mask | Specifies the subnet mask of the RTP stream being filtered. |

This command has no default settings.

Command mode

This example shows how to enable RTP stream filtering:

root@localhost# monitor rtp-stream filter 1.2.3.0 255.255.255.0 4.5.0.0 255.255.0.0

**metric export host**

# monitor rtp-stream threshold

To set the alarm threshold for the different RTP stream monitoring types, use the monitor rtp-stream threshold command. To disable the alarm threshold RTP stream monitoring, use the no form of this command.

monitor rtp-stream **threshold** <key\_word>

no monitor rtp-stream **threshold** <key\_word>

|  |  |
| --- | --- |
| Key Word | Action |
| actual-pkt-loss | Specifies the actual packet loss percentile threshold and enables the actual packet loss threshold alarm.  |
| **adjusted-pkt-loss** | Specifies the adjusted packet loss percentile threshold and enables the adjusted packet loss threshold alarm.  |
| **jitter** | Specifies the jitter alarm threshold and enables the jitter threshold alarm in milliseconds. |
| **mos** | Specifies the MOS score threshold and enables the MOS score alarm. |
| **soc** | Specifies the seconds of concealment threshold and enables the soc alarm.  |
| ssc | Specifies the severe seconds of concealment threshold and enables the ssc alarm.  |

This command has no default settings.

Command mode

This command is supported on all NAM platforms.

This example shows how to set an alarm threshold of 6% for RTP stream monitoring of lost packets.

root@NAM.cisco.com# monitor rtp-stream threshold adjusted-pkt-loss 6

Successfully set adjusted-pkt-loss alarm.

root@NAM.cisco.com#

# monitor urlcollection

To enter the URL collection submode and configure URL collection, use the monitor urlcollection command. To disable the URL collection, use the no form of this command.

monitor urlcollection

no monitor urlcollection

This command has no keywords or arguments.

This command has no default settings.

Command mode

When you enter the URL collections submode, the following commands are available:

* **?** or **help**—Displays help; see the **help** command.
* **cancel**—Discards changes and exits from the subcommand mode; see the **autocreate-data-source** command section.
* **data-source** nam-data-source-name—Specifies the NAM data source name.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **ignore**—(Optional) Sets the host, path, and the URL matching argument.
* **ignore** host—Specifies that you ignore or do not ignore the URL’s host part when collecting URL collection data.
* **ignore** path—Specifies that you ignore or do not ignore the URL’s parth part when collecting URL collection data.
* **ignore** url-arg—Specifies that you ignore or do not ignore the URL’s arguments when collecting URL collection data.
* **ignore** enable | disable—Enables or disables this command.
* **match-only** string—(Optional) Specifies collecting only the URL data that matches the string in the URL.
* **max-entry** 100 | 50 | 1000—(Optional) Specifies the maximum of URL collection entries.
* **recycle** enable | disable—Enables or disables aging of the URL collection data entries.

There is only one URL collection in NAM. The collection owner is always LocalMgr. The index is always one.

This example shows how to configure URL collection:

root@localhost# monitor urlcollection

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@localhost(sub-monitor-url-collection)# ?

? - display help

cancel - discard changes and exit from subcommand mode

data-source - specify the collection data source (\*)

exit - exit from the subcommand mode

help - display help

ignore - set url collection data matching schemes

match-only - match string for url collection data

max-entry - set max number data entries of url collection

recycle - enable or disable aging of url collection data entries

(\*) - denotes a mandatory field for this configuration.

root@localhost(sub-monitor-url-collection)#

**show monitor urlcollection**

# monitor urlfilter

To enter the URL filter collection configuration subcommand mode, and then configure URL filters, use the monitor urlfilter command. To remove the URL filters from the configuration, use the no form of this command. This command is removed in NAM 6.0(1).

monitor urlfilter

no monitor urlfilter control-index

|  |  |
| --- | --- |
| control-index | Specifies the collection control index. Range is from 1 to 65535. |

The control index is random.

Command mode

When you enter the monitor URL filter subcommand mode, the following commands are available:

* **?**—Displays help.
* **cancel**—Discards changes and exits from the subcommand mode.
* **control-index** control-index—Specifies the URL entry’s control index. Range is from 1 to 65535. Default is random.
* **description** string—(Optional) Specifies the URL filter’s description string.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **help**—Displays help.
* host-regexp—Specifies the regular expression for the URL’s host.
* path-regexp—Specifies the regular expression of the URL’s path.
* protocol-encap—(Optional) Specifies the protocol encapsulation of the HTTP packet.

The clear configuration command removes the URL filters from the configuration. There is no SNMP support for configuring the URL filters.

This example shows how to configure URL filters:

root@nam# monitor urlfilter

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@nam(sub-monitor-url-filter)# control-index 2

root@nam(sub-monitor-url-filter)# description urlfilter example

root@nam(sub-monitor-url-filter)# host-regexp www.example.com

root@nam(sub-monitor-url-filter)# protocol-encap ipv4

root@nam(sub-monitor-url-filter)# exit

Sucessfully created urlfilter entry.

root@nam# show monitor urlfilter

Description: urlfilter example

 Control index: 2

 Protocol encapsulation: IPv4

 URL's host string: www.example.com

 URL's path string: (not-set)

To remove this URL filter entry, use the no form of the command:

root@nam# no monitor urlfilter 2

Successfully delete urlfilter entry.

**show monitor urlfilter**

# mtrace-clear, mtrace-show, mtrace-start, mtrace-stop, mtrace-upload

These are memory debug commands. They are not for NAM feature use. Please do not use without request from NAM support engineers.

mtrace-clear

mtrace-show

mtrace-start

mtrace-stop

mtrace-upload *url-path*

The first four commands have no arguments or keywords. mtrace-upload needs FTP pathname for mtrace upload

These commands have no default settings.

Command mode

# netflow input port

To set a specified value of the input NetFlow UDP port on NAM, use the **netflow input port** [port] command.

netflow input port [port]

* In case this CLI is not used, NAM retains the default port 3000 to listen to incoming NDEs. When invoked, the CLI prints both old and new UDP port numbers, if successfully completed.

|  |  |
| --- | --- |
| port | Specifies the input UDP port number, valid values 1 - 65535. |

The default port is 3000.

Command mode

This example shows how to use the **netflow input port** command.

root@localhost# **netflow input port 9101**

NetFlow input port 3000 changed to 9101

# nslookup

To configure name server queries, use the nslookup command.

nslookup hostname [server]

|  |  |
| --- | --- |
| hostname | Specifies the name server query host. |
| server | (Optional) Specifies the name server to query. |

This command has no default settings.

Command mode

This example shows how to configure name server queries:

root@localhost.cisco.com# nslookup www.yahoo.com

Server: 127.0.0.1

Address: 127.0.0.1#53

Non-authoritative answer:

www.yahoo.com canonical name = www.yahoo.akadns.net.

Name: www.yahoo.akadns.net

Address:66.218.71.80

root@localhost.cisco.com#

# password

To set a new password, use the password command.

password username

|  |  |
| --- | --- |
| username | Sets the user login name whose password will be changed. |

This command has no default settings.

Command mode

There are only two valid users, root and guest.

This example shows how to set a password:

root@localhost.cisco.com# password root

Changing password for user root

New UNIX password:

Retype new UNIX password:

passwd:all authentication tokens updated successfully

root@localhost.cisco.com#

# password strong-policy

To enable strong password policy for user names, use the password strong-policy command. To disable this option, use the **no** form of this command.

password strong-policy

no password strong-policy

This command has no default settings.

Command mode

There are only two valid users, root and guest.

This example shows how to set a password:

root@localhost.cisco.com# password strong-policy

Strong password policy is enabled.

# patch

To download and install a software patch, use the patch command.

patch ftp://user:passwd@host/full-path/filename

|  |  |
| --- | --- |
| ftp://user:passwd@host/full-path/filename | Sets the path to download the patch. |

This command has no default settings.

Command mode

This example shows how to download and install a patch:

root@localhost.cisco.com# patch ftp://hostname/fullpath/c6nam-3.6-strong-cryptoK9-patch-1-0.bin

Proceeding with installation. Please do not interrupt.

If installation is interrupted, please try again.

Downloading c6nam-3.6-strong-cryptoK9-patch-1-0.bin. Please wait...

ftp://hostname/fullpath/c6nam-3.6-strong-cryptoK9-patch-1-0.bin (1K)

- [########################] 1K | 1886.33K/s

1891 bytes transferred in 0.00 sec (1569.00k/sec)

Verifying c6nam-3.6-strong-cryptoK9-patch-1-0.bin. Please wait...

Patch c6nam-3.6-strong-cryptoK9-patch-1-0.bin verified.

Applying /usr/local/nam/patch/workdir/c6nam-3.6-strong-cryptoK9-patch-1-0.bin. Please wait...

########################################### [100%]

########################################### [100%]

Patch applied successfully.

root@localhost.cisco.com#

**show patches**

**show version**

# pid-sn

To enter the Product ID and Serial number of a WAE device for node locking with a NAM Virtual Blade product license, use the pid-sn command. This command is removed in NAM 6.0(1).

pid-sn PIDnnnn SNnnnn

|  |  |
| --- | --- |
| **PIDnnnn** | Specifies the Product ID of the WAE device.  |
| **SNnnnn** | Specifies the serial number of the WAE device.  |

This command has no default settings.

Command mode

This command is valid only on NAM Virtual Blade platforms.

This example shows how to ener the Product ID and serial number of a WAE device:

root@localhost# pid-sn WAE-674-K9 KXQCDHDR

root@localhost#

# ping

To check connectivity to a IPv4 network device, use the ping command.

ping [-n | -v] [-c count] [-i wait] [-p pattern] [-s packetsize] hostname | IP address

|  |  |
| --- | --- |
| **-n** | (Optional) Displays the network addresses as numbers. |
| **-v** | (Optional) Specifies verbose output. |
| **-c count** | (Optional) Stops the ping after sending the count of ECHO\_REQUEST packets. |
| **-i wait** | (Optional) Specifies the time interval in seconds between sending each packet. |
| **-p pattern** | (Optional) Specifies the pad bytes to fill out packets sent in the ping. You may specify up to 16 pad bytes to fill out packets being sent. |
| **-s packetsize** | (Optional) Sets the 8 bytes of ICMP header data. |
| **hostname** | Sets the hostname of the network device to ping. |
| **IP address** | Specifies the IP address of the network device to ping. |

This command has no default settings.

Command mode

This example shows how to check the connectivity of a network device with ping:

root@localhost# ping -n -v ralph 100.20.19.23

root@localhost#

# ping6

To check connectivity to a IPv6 network device, use the ping6 command. This command was introduced in NAM 6.0(1).

Ping6 [-n | -v] [-c count] [-i wait] [-p pattern] [-s packetsize] [-I interface] [-M hint] hostname | IP address

|  |  |
| --- | --- |
| **-n** | (Optional) Displays the network addresses as numbers. |
| **-v** | (Optional) Specifies verbose output. |
| **-c count** | (Optional) Stops the ping6 after sending the count of ECHO\_REQUEST packets. |
| **-i wait** | (Optional) Specifies the time interval in seconds between sending each packet. |
| **-p pattern** | (Optional) Specifies the pad bytes to fill out packets sent in the ping. You may specify up to 16 pad bytes to fill out packets being sent. |
| **-s packetsize** | (Optional) Sets the 8 bytes of ICMP header data. |
| **-I interface** | (Optional)Sets the name of the specific interface. When pinging IPv6Link-local address this option is required. |
| **-M hint** | (Optional)Select Path MTU Discovery strategy. **hint** may be do prohibit fragmentation. Want do PMTU discovery, fragment locally when packet size is large. Do not set DF flag. |

This command has no default settings.

Command mode

This example shows how to check the connectivity of a network device with ping6:

# ppack

The ppack command allows you to upload a protocol pack to the NAM or set the current protocol pack back to the default. This command was introduced in NAM 6.1(1) release.

ppack load <url>

ppack restore-default

This command has no default settings.

Command mode

Examples

ppack restore-default – will restore the default protocol pack

ppack load ftp://1.2.3.4/path/to/the/protocol/pack -- will load the protocol pack in the url

# preferences

To enter the preferences subcommand mode, and then configure how your screen displays information, use the preferences command.

preferences

This command has no arguments or keywords.

This command has no default settings.

Command mode

When you enter the preferences subcommand mode, the following commands are available:

* **cancel**—Discards changes and exits from the subcommand mode.
* **csv-export all** | **current-screen**—Sets the comma-separated values export monitor data options.
* **data-displayed** bits | **bytes**—Specifies how the data is displayed in bits or bytes. **entries-per-screen** 1-100—(Optional) Sets the number of rows to display in tabular screens. Default is 15. This is removed in NAM 6.0(1).
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **format-large-number enable** | **disable**—Displays the GUI counters in large numbers: K(kilo), M(mega), or G(giga). This is removed in NAM 6.0(1).
* **graph-bars** 1-15— (Optional) Sets the number of bars on a displayed graph. Default is 10.
* **help**—Displays help; see the **help** command.
* **number-notation commas-dot** | **dots-comma** | s*paces-comma*—Sets the number notation to commas or dot and so forth. For example: 1,000 or 1.000 or 300, 10.
* **refresh-interval** 60-3600—(Optional) Sets the screen refresh interval in seconds. Default is 60. This is changed from 15 – 3600.
* **rsptime**-displayed – Sets the response time display unit option (as of NAM 6.1(1))
	+ **automatic** – Sets the display unit to automatic
	+ **microseconds** – Sets microseconds as the response time display unit
	+ **milliseconds** – Sets milliseconds as the response time display unit
	+ **seconds** – Sets seconds as the response time display unit
* **resolve-hostname** enable | disable—(Optional) Enables or disables hostname resolution. Default is enable.
* **Audit-trail** enable | disable—Enables or disables audit trail. This was introduced in NAM 6.0(1).
* **Capture-format enc**—set enc as capture format. This was introduced in NAM 6.0(1).
* **Capture-format pcap**—set pcap as capture format. This was introduced in NAM 6.0(1).

This example shows how to configure preferences for your screen display:

root@nam.localdomain# preferences

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@nam.localdomain(sub-preferences)# audit-trail enable

root@nam.localdomain(sub-preferences)# capture-format enc

root@nam.localdomain(sub-preferences)# data-displayed bytes

root@nam.localdomain(sub-preferences)# graph-bars 10

root@nam.localdomain(sub-preferences)# number-notation commas-dot

root@nam.localdomain(sub-preferences)# refresh-interval 60

root@nam.localdomain(sub-preferences)# resolve-hostname enable

root@nam.localdomain(sub-preferences)# exit

NAM web interface preferences updated successfully.

This example shows how to display the configured preferences:

root@nam.localdomain# show preferences

Refresh interval: 60 secs

Number of graph bars: 10

Hostname resolution: Enabled

Data displayed in: Bytes

Number notation: Commas-dot

Audit trail: Enabled

Capture format: ENC

**show preferences**

# protocol esp-null-heuristic

Use the protocol esp-null-heuristic command to enable and disable the NAM to parse ESP-NULL protocol heuristically.

To enable the NAM to parse ESP-NULL protocol heuristically, use the following command:

**protocol esp-null-heuristic enable**

To disable the NAM to parse ESP-NULL protocol heuristically, use the following command:

no protocol esp-null-heuristic enable

This command enables and disables heuristic parsing of ESP-NULL packets.

This command has no default settings.

Command mode

This example shows how to enable parsing heuristically:

root@localhost# protocol esp-null-heuristic enable

root@localhost#

This example shows how to disable parsing heuristically:

root@localhost# no protocol esp-null-heuristic enable

root@localhost#

# reboot

To shut down and then restart NAM, use the reboot command.

reboot

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to reboot the NAM:

root@localhost# reboot

Reboot the NAM? (Y/N) [N]:

root@localhost#

# reboot -helper

To reboot to helper image, use the reboot -helper command.

reboot -helper

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to reboot to helper image:

root@localhost# reboot -helper

Reboot the NAM? (Y/N) [N]:

root@localhost#

# reboot -golden

To reboot to the golden helper image (NAM-3), use the reboot -golden command.

reboot -golden

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to reboot to helper image:

root@localhost# reboot -golden

Reboot the NAM? (Y/N) [N]:

root@localhost#

# remote-storage

**remote-storage fcoe**

**remote-storage iscsi**

**remote-storage sas**

# remote-storage fcoe

To list or format the FCoE remote storage targets for capture data, use the remote-storage fcoe command.

remote-storage fcoe

|  |  |
| --- | --- |
| name | Specifies the name for the FCoE remote storage being removed. |

This command has no default settings.

Command mode

These commands are supported only on NAM-3.

When you enter the command, the following are available:

* **format**—Formats one or more FCoE storage targets.
* **fsck**—Runs FS check on a FCoE storage target (may take several minutes).
* **label**—Labels a FCoE storage target.
* **list**—Lists all the FCoE storage targets.
* local-pwwn—Shows local FCoE Port WWN. Use the storage vendor's web interface to map the NAM local ID to the storage LUNs.
* mount—Reconnects a logically disconnected FCoE storage target. Replaces connect command.
* refresh—Refreshes the FCoE service.
* **sfp-info**—Displays important information from the SFP and module EEPROM, including type, vendor, part number, serial number, and data code.
* **unmount**—Logically disconnects a FCoE storage target (so it can be safely removed). Replaces disconnect command.

This example shows how to configure a remote storage for capturing FCoE data:

root@hostname.cisco.com# remote-storage fcoe

format - format one or more FCoE storage targets

fsck - run FS check on a FCoE storage target (may take several minutes)

label - label a FCoE storage target

list - list all FCoE storage targets

local-pwwn - show local FCoE Port WWN

mount - re-mount a FCoE storage target

refresh - refresh the FCoE service

sfp-info - display SFP+ EEPROM contents

unmount - unmount a FCoE storage target (safely remove)

root@hostname.cisco.com#

# remote-storage iscsi

To list or format the iSCSI remote storage targets for capture data, use the remote-storage iscsi command.

remote-storage iscsi

|  |  |
| --- | --- |
| name | Specifies the name for the iSCSI remote storage being removed. |

* This command is not supported on the NAM WAAS Virtual Blade.

This command has no default settings.

Command mode

When you enter the command, the following are available:

* format—Formats a iSCSI storage target.
* fsck—Runs FS check on an iSCSI storage target (may take several minutes).
* label —Labels an iSCSI storage target.
* list—Lists all iSCSI storage targets.
* local-iqn—Shows local iSCSI Qualified Name. Use the storage vendor's web interface to map the NAM local ID to the storage LUNs.
* login—Logs into an iSCSI session.
* logout—Logs out from an iSCSI session.
* mount—Re-mounts an iSCSI storage target.
* unmount—Unmounts an iSCSI storage target (so it can be safely removed).
* discover—discover targets at a given IP address. This was introduced in NAM 6.0(1).

This example shows how to configure a remote storage for capturing iSCSI data:

root@hostname.cisco.com# remote-storage iscsi

format - format a iSCSI storage target

fsck - run FS check on an iSCSI storage target (may take several minutes)

label - label an iSCSI storage target

list - list all iSCSI storage targets

local-iqn - show local iSCSI Qualified Name

login - Login to an iSCSI session

logout - Logout from an iSCSI session

mount - re-mount an iSCSI storage target

unmount - unmount an iSCSI storage target (safely remove)

discover - discover targets at a given IP address

root@hostname.cisco.com#

This example shows the output of remote-storage iscsi local-iqn:

root@hostname.cisco.com# remote-storage iscsi local-iqn

Local iSCSI Qualified Name: iqn.1987-05.com.cisco:WS-SVC-NAM3-6G-K9.00:19:55:07:14:FA

The example shows the output of remote-storage iscsi list. It includes a list of iSCSI sessions at the end.

root@hostname.cisco.com# remote-storage iscsi list

Storage ID: 7

Label:

Status: Ready

Protocol: ISCSI

Target IP: 172.20.98.182

Target IQN: iqn.1999-02.com.nexsan:p0:satabeast2:029c65ec

Type: LUN

Model: NEXSAN SATABeast2

LUN: 2

Capacity: 1.82TB

Available: 1.73TB

Active iSCSI Sessions:

tcp: [2] 172.20.98.182:3260,1 iqn.1999-02.com.nexsan:p0:satabeast2:029c65ec

root@hostname.cisco.com#

**show remote-storage**

# remote-storage sas

To list or format the SAS remote storage targets for capture data, use the remote-storage sas command.

remote-storage sas

|  |  |
| --- | --- |
| name | Specifies the name of the SAS remote storage being removed. |

This command has no default settings.

Command mode

These commands are supported only on NAM-3.

When you enter the command, the following are available:

* **format**—Format one or more SAS storage targets.
* **fsck**—Run FS check on a SAS storage target (may take several minutes).
* **label**—Label a SAS storage target.
* **list**—List all the SAS storage targets.
* **local-address**—Show local SAS address. Use the storage vendor's web interface to map the NAM local ID to the storage LUNs.
* **mount**—Reconnects a logically disconnected SAS storage target. Replaces connect command.
* **unmount**—Disconnects a SAS storage target (so it can be safely removed). Replaces disconnect command.

This example shows how to configure a remote storage for capturing SAS data:

root@hostname.cisco.com# remote-storage sas

fsck - run FS check on a SAS storage target (may take several minutes)

format - format one or more SAS storage targets

label - label a SAS storage target

list - list all SAS storage targets

local-address - show local SAS Address

mount - re-mount a SAS storage target

unmount - unmount a SAS storage target (safely remove)

# remove corefiles

To remove all existing core files, use the remove corefiles command. This was introduced in NAM 6.0(1).

Remove corefiles

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to remove all existing core files:

root@nam.localdomain# remove corefiles

root@nam.localdomain#

**show corefiles**

# rise-nam enable / disable

To enable or disable nam rise interface, use the rise-nam enable / disable command. This was introduced in NAM 6.0(2) and currently only works on NAM 2300 appliances.

rise-nam enable | disable

|  |  |
| --- | --- |
| **disable** | disable RISE for NAM appliance.  |
| **enable** | enable RISE for NAM appliance.  |

default is disable for 6.0(2).

Command mode

These examples show how to enable and disable rise interface on NAM appliances:

root@nam.localdomain# rise-nam enable

root@nam.localdomain# rise-nam disable

# rmwebusers

To remove all web users from the local web user database, use the rmwebusers command.

rmwebusers

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to remove web users from the local web user database:

root@localhost.cisco.com# rmwebusers

WARNING:Doing this will stop the web server and remove

all locally defined web users from web user database.

Are you sure you want to continue (y/n) [n]? y

Disabling HTTP server...

Successfully disabled HTTP server.

All locally defined web users have been

removed from web user database.

root@localhost.cisco.com#

**show web-user**

# secure-clear all

To clean all users data before shipping, use the secure-clear all command. This was introduced in NAM 6.0(1).

Secure-clear all

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to clean all users data before shipping:

root@nam.localdomain# secure-clear all

This operation will erase completely NAM user data.

(including removing the NAM IP connectivity parameters such

as IP address, To reconfigure the NAM network connectivity,

you must use the switch/router session CLI command or UART port.

Do you wish to continue? (y/n) [n]:

# show access-log

To display the web access log, use the show access-log command.

show access-log

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the web access log:

Root@localhost# show access-log

11 Mar 2003, 12:23:38 152.20.27.182 - Access denied (no login session)

 /error.php

11 Mar 2003, 12:23:39 152.20.27.182 - Access denied (no login session)

 /error.php

11 Mar 2003, 12:23:39 152.20.27.182 - Access denied (no login session)

 /error.php

11 Mar 2003, 12:23:39 152.20.27.182 - Access denied (no login session)

 /error.php

# show application app-id

To display all applications, use the show application app-id command.

show application **app-id**

This command has no default settings.

Command mode

This example shows how to display all applications:

root@NAM.cisco.com# **show application app-id**

sample-l3:1 (16777217) icmp

sample-l3:2 (16777218) igmp

sample-l3:4 (16777220) ip

sample-l3:6 (16777222) tcp

sample-l3:8 (16777224) egp

**application**

# show application eng-id

To display application information per engine ID, use the show application eng-id command.

show application **eng-id**

This command has no default settings.

Command mode

This example shows how to display application information per engine ID:

root@NAM.cisco.com# **show application eng-id 1**

sample-l3:1 (16777217) icmp

sample-l3:2 (16777218) igmp

sample-l3:4 (16777220) ip

sample-l3:6 (16777222) tcp

sample-l3:8 (16777224) egp

**application**

# show application group

To display application groups, use the show application group command.

show application **group** [group-name]

|  |  |
| --- | --- |
| group-name | (Optional) Specifies the application group name. |

This command has no default settings.

Command mode

This example shows how to display application groups:

root@namlab-kom10.cisco.com# show application group

Application Group: File-Transfer

 Number of Protocols: 5

 - ftp

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.21.4.0.1.0.0

 - ftp-data

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.20.4.0.1.0.0

 - ftps

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.222.4.0.1.0.0

 - ftps-data

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.221.4.0.1.0.0

 - tftp

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.69.4.0.1.0.2

Application Group: Peer-to-Peer

 Number of Protocols: 12

 - gnutella(6346)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.24.202.4.0.1.0.0

 - gnutella(6347)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.24.203.4.0.1.0.0

 - fasttrack(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.4.190.4.0.1.0.0

 - fasttrack(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.4.190.4.0.1.0.0

 - winmx(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.24.113.4.0.1.0.

 - winmx(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.26.43.4.0.1.0.0

 - edonkey(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.18.57.4.0.1.0.0

 - edonkey(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.18.53.4.0.1.0.0

 - hotline

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.21.124.4.0.1.0.0

 - soulseek

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.8.186.4.0.1.0.0

 - directconnect

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.155.4.0.1.0.0

 - bittorrent

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.26.225.4.0.1.0.0

Application Group: Web

 Number of Protocols: 2

 - http

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.80.4.0.1.0.0

 - https

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.187.4.0.1.0.0

Application Group: Database

 Number of Protocols: 9

 - sql\*net

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.66.4.0.1.0.0

 - sqlserv(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.118.4.0.1.0.0

 - sqlserv(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.118.4.0.1.0.0

 - ms-sql-mon(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.5.154.4.0.1.0.0

 - ms-sql-mon(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.154.4.0.1.0.0

 - ms-sql-ser(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.5.153.4.0.1.0.0

 - ms-sql-ser(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.153.4.0.1.0.0

 - oracle-server(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.5.245.4.0.1.0.0

 - oracle-server(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.245.4.0.1.0.0

Application Group: email

 Number of Protocols: 7

 - smtp

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.25.4.0.1.0.0

 - smtps

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.209.4.0.1.0.0

 - pop3(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.110.4.0.1.0.0

 - pop3(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.110.4.0.1.0.0

 - pop3s

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.227.4.0.1.0.0

 - imap2

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.143.4.0.1.0.0

 - imaps

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.225.4.0.1.0.0

Application Group: Multi-Media

 Number of Protocols: 9

 - h225

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.184.4.0.1.0.0

 - h245

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.182.4.0.1.0.0

 - h323-gatekeeper

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.6.183.4.0.1.0.0

 - rtp

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.125.0.4.0.1.0.0

 - rtcp

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.125.1.4.0.1.0.0

 - sip(udp)

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.19.196.4.0.1.0.

 - sip(tcp)

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.19.196.4.0.1.0.0

 - mgcp

 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.9.123.4.0.1.0.0

 - sccp

 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.7.208.4.0.1.0.0

**application**

# show audit-trail

To display the audit trail configuration, use the show audit-trail command.

show audit-trail

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the audit trail configuration:

root@hostname.cisco.com# show audit-trail

Audit trail is enabled.

root@hostname.cisco.com#

**audit-trail enable**

# show autocreate-data-source

To display the autocreated data-sources, use the **show autocreate-data-source** command.

show autocreate-data-source

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows if the autocreation of data-sources feature is enabled:

root@NAM.cisco.com# show autocreate-data-source

NDE autocreation : ENABLED

WAAS autocreation : ENABLED

ERSPAN autocreation : ENABLED

Autocreate WAAS Client data source : ENABLED

Autocreate WAAS Client WAN data source : DISABLED

Autocreate WAAS Server WAN data source : DISABLED

Autocreate WAAS Server data source : DISABLED

Autocreate WAAS Passthru data source : DISABLED

Enable Passthru export on autocreated WAAS device : NO

root@NAM.cisco.com#

# show cdb

To display information about a CDB file, use the show cdb command. Since NAM 6.0(1), this command has been changed from show cdb [filename] to the specific cdb names.

show cdb [filename]

show cdb ARTCltSvr

show cdb ARTSiteClt

show cdb ARTSiteClt\_lt

show cdb ARTSiteSvr

show cdb ARTSiteSvr\_lt

show cdb AlarmMessages

show cdb CoreConv

show cdb DataSourceStats

show cdb DataSourceStats\_lt

show cdb Hosts

show cdb Hosts\_lt

show cdb MDIfStats

show cdb MDIfStats\_lt

show cdb RtpConv

show cdb RtpMos

show cdb RtpMos\_lt

show cdb SiteStats

show cdb SiteStats\_lt

show cdb SiteMatrix

show cdb SiteMatrix\_lt

show cdb VoIPCalls

show cdb file-list

|  |  |
| --- | --- |
| FilenameARTCltSvrARTSiteCltARTSiteClt\_ltARTSiteSvrARTSiteSvr\_ltAlarmMessagesCoreConvDataSourceStatsDataSourceStats\_ltHostsHosts\_ltMDIfStatsMDIfStats\_ltRtpConvRtpMosRtpMos\_ltSiteMatrix*SiteMatrix\_lt**SiteStats**SiteStats\_lt**VoIPCalls**file-list* | Specifies the CDB filename.IAP Client-Server tableIAP Site-Client tableIAP Site-Client Long-Term tableIAP Site-Server tableIAP Site-Server Long-Term tableAlarm Messages tableConversation tableData Source Stats tableData Source Stats Long-Term tableHost tableHost Long-Term tableManaged Device Interface Stats tableManaged Device Interface Stats Long-Term tableRTP Stream tableRTP MOS Quality tableRTP MOS Quality Long-Term tableSite Matrix tableSite Matrix Long-Term tableSite Stats tableSite Stats Long-Term tableVoice Signaling Data tableList CDB files |

This command has no default settings.

Command mode

This example shows how to display information about a CDB file:

root@nam.localdomain# show cdb

<FILENAME> - File to examine (e.g. Hosts)

ARTCltSvr - IAP Client-Server table

ARTSiteClt - IAP Site-Client table

ARTSiteClt\_lt - IAP Site-Client Long-Term table

ARTSiteSvr - IAP Site-Server table

ARTSiteSvr\_lt - IAP Site-Server Long-Term table

AlarmMessages - Alarm Messages table

CoreConv - Conversation table

DataSourceStats - Data Source Stats table

DataSourceStats\_lt - Data Source Stats Long-Term table

Hosts - Host table

Hosts\_lt - Host Long-Term table

MDIfStats - Managed Device Interface Stats table

MDIfStats\_lt - Managed Device Interface Stats Long-Term table

RtpConv - RTP Stream table

RtpMos - RTP MOS Quality table

RtpMos\_lt - RTP MOS Quality Long-Term table

SiteMatrix - Site Matrix table

SiteMatrix\_lt - Site Matrix Long-Term table

SiteStats - Site Stats table

SiteStats\_lt - Site Stats Long-Term table

VoIPCalls - Voice Signaling Data table

file-list - List CDB files

# show cdp settings

To display the current Cisco Discovery Protocol (CDP) settings, use the show cdp settings command.

show cdp settings

* This command is not supported on NAM-1 or NAM-2 devices or the NAM Virtual Blade.

This command has no arguments or keywords.

This command has no default settings.

Command mode

This command is supported only on NME-NAM-80S and NME-NAM-120S devices and Cisco NAM 2200 Series appliances.

To display the current CDP settings:

root@nam# show cdp settings

CDP is disabled

 Message Interval: 60

 Message Hold Time: 180

root@nam#

**autocreate-data-source**

**cdp hold-time**

**cdp interval**

# show certificate

To display the installed certificate, use the show certificate command.

show certificate

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display certificate information:

Root@localhost# show certificate

-----BEGIN CERTIFICATE-----

MIIDgzCCAuygAwIBAgIBADANBgkqhkiG9w0BAQQFADCBjjELMAkGA1UEBhMCVVMx

CzAJBgNVBAgTAkNBMQswCQYDVQQHEwJTSjEbMBkGA1UEChMSQ2lzY28gU3lzdGVt

cywgSW5jMSswKQYDVQQLEyJDYXRhbHlzdCA2MDAwIE5BTSBUZXN0IENlcnRpZmlj

YXRlMRswGQYDVQQDExJDaXNjbyBTeXN0ZW1zLCBJbmMwHhcNMDExMTI3MTI0MDIw

WhcNMDYxMTI2MTI0MDIwWjCBjjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQsw

CQYDVQQHEwJTSjEbMBkGA1UEChMSQ2lzY28gU3lzdGVtcywgSW5jMSswKQYDVQQL

EyJDYXRhbHlzdCA2MDAwIE5BTSBUZXN0IENlcnRpZmljYXRlMRswGQYDVQQDExJD

aXNjbyBTeXN0ZW1zLCBJbmMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMfd

NQJunHkjduRGMc7B978Bgh4xlEixRCPQ9K74PNzmXbZlIayRUXvLHA3xCM8GamFt

SlLgjO5R3q0cHWnUrluknHeI1UfZMQMiL0IqL255JxX6NbvCUzGpTxNMKywDXDc3

VevqmPezWrHAFxx3hoXtgTnj6j6BMxyOkbYDwAFXAgMBAAGjge4wgeswHQYDVR0O

BBYEFPNCoN6ndQG9nCmgnzP+Y3VxOSP3MIG7BgNVHSMEgbMwgbCAFPNCoN6ndQG9

nCmgnzP+Y3VxOSP3oYGUpIGRMIGOMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0Ex

CzAJBgNVBAcTAlNKMRswGQYDVQQKExJDaXNjbyBTeXN0ZW1zLCBJbmMxKzApBgNV

BAsTIkNhdGFseXN0IDYwMDAgTkFNIFRlc3QgQ2VydGlmaWNhdGUxGzAZBgNVBAMT

EkNpc2NvIFN5c3RlbXMsIEluY4IBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEB

BAUAA4GBAD95psLs1tneBsIuUWQvIdV6D7QYBfewtDzNW10lFvgDZBQdIu7QeRtL

tjMNyGDUIG7tz7/9iZyA90rfrkM410qJrJysoKBZgMzTg6ilpaIzPnoJnN4DYj5C

qNGuOM0OKqtpqCFMKq87UXUuvTgc3hhQKSY5LKOXhJyhtCupJ669

-----END CERTIFICATE-----

**show certificate-request**

# show certificate-request

To display the certificate-signing requests, use the show certificate-request command.

show certificate-request

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the certificate-signing requests:

Root@localhost# show certificate-request

**show certificate**

# 5: NAM CLI Commands: show classification-settings to show monitor urlfilter

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter describes the following NAM CLI commands: “show classification-settings” to “show monitor urlfilter”.

# show classification-settings

To show current packet classification setting on the NAM, use the show classification-settings command. This command was introduced in NAM 6.0(1).

show classification-settings

This command has no arguments or keywords.

This command has no default settings.

Command mode

The following example shows how to display current packet classification settings.

root@nam.localdomain# show classification-settings

Classification method: Default

root@nam.localdomain#

# show cli

To display the CLI configuration, use the **show cli** command. This command was introduced in NAM 6.1(1).

**show cli**

This command has no arguments or keywords.

This command has no default settings.

Command mode

The following example shows how to display cli timeout settings.

root@nam.localdomain# show cli

Idle/inactivity timeout: disabled

root@nam.localdomain#

**Related Commands**

cli idle-timeout

# show clock details

To show clock details on the NAM, use the show clock details command.

show clock details

This command has no arguments or keywords.

This command has no default settings.

Command mode

The following example shows how to display clock settings.

root@nam.cisco.com# show clock details

System Time: Thu Nov 4 18:25:41 PDT 2010

# show configuration

To display the NAM running configuration, use the show configuration command.

show configuration

This command has no arguments or keywords.

This command has no default settings.

Command mode

The following configurations are not included in the generated configuration file:

* Reports
* CLI users
* Supervisor engine community strings

This example shows how to display the NAM running configuration:

Root@localhost# show configuration

\*\*\*\*\* NAM configuration \*\*\*\*\*

Time: Tue Apr 26 00:10:31 2011

preferences

 entries-per-screen 15

 refresh-interval 60

 graph-bars 0

 resolve-hostname disable

 data-displayed bits

 format-large-number disable

 number-notation commas-dot

 csv-export all

 exit

!

monitor art response-times

 report-interval 1800

 rsp-time1 1

 rsp-time2 5

 rsp-time3 10

 rsp-time4 50

 rsp-time5 100

 rsp-time6 500

 rsp-timeout 1000

 exit

!

**Related Commands**

**config clear**

# show corefiles

To display the corefiles, use the show corefiles command. This command was introduced in NAM 6.0(1).

show corefiles

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display corefiles:

root@nam.localdomain# show corefiles

root@nam.localdomain#

**Related Commands**

**remove corefiles**

# show counters

To display the counters for data aggregation table, use the show counters command.

show counters

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the counters for data aggregation table:

root@nam235Cat6k.cisco.com# show counters ?

classification - show classification engine counters (as of NAM 6.1(1))

long-term - show long-term collection counters

nde-export - show collection counters for NDE export

nde-receive - show collection counters for NDE receive (as of NAM 6.1(1))

short-term - show short-term collection counters

# show cpu

To display the Central Processing Unit (CPU) utilization, use the show cpu command.

show cpu

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the CPU utilization:

root@nam235Cat6k.cisco.com# **show cpu**

NOTE: For more details on system resources including CPU

utilization, visit the Administration -> System -> Resources

page in the NAM Traffic Analyzer web application.

root@nam235Cat6k.cisco.com#

# show data-source

To display the data-sources, use the show data-source command.

show data-source

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the data-sources:

root@nam235Cat6k.cisco.com# **show data-source**

DATA SOURCE ID : 1

DATA SOURCE NAME : DATA PORT 1

TYPE : Data Port

PORT NUMBER : 1

-----------

DATA SOURCE ID : 2

DATA SOURCE NAME : DATA PORT 2

TYPE : Data Port

PORT NUMBER : 2

-----------

# show date

To display the current date and time, use the show date command.

show date

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the current date and time:

Root@localhost# show date

Tue Apr 26 00:14:18 2011

**show time**

**time**

# show debug log-levels

To display log level settings, use the show debug log-levels command.

show debug log-levels

This command has no arguments or keywords.

This command has no default behavior or settings.

Command mode

The following example shows log level settings:

root@nam.cisco.com# **show debug log-levels**

Debug Logging: enabled

Feature OTHER (1): error (1)

Feature POLLD (3): error (1)

Feature SWPOLLD (4): error (1)

Feature TREND\_DAEMON (5): error (1)

Feature TREND\_RPC (6): error (1)

Feature TREND\_SNMP (7): error (1)

Feature MAIN (8): error (1)

Feature MISC (9): error (1)

Feature SNMP (10): error (1)

Feature SRSNMP (11): error (1)

Feature ENTITY (12): error (1)

Feature RMON (13): error (1)

Feature RPC (14): error (1)

Feature DSRC (15): error (1)

Feature WAAS (16): error (1)

Feature PARSER (17): error (1)

Feature PPROC (18): error (1)

Feature FM (19): error (1)

Feature FR (20): error (1)

Feature COLL\_SHARED (21): error (1)

Feature RTP (22): error (1)

Feature METRIC\_ENGINE (23): error (1)

Feature ART (24): error (1)

Feature URL\_COLLECTION (25): error (1)

Feature PORT\_TABLE (26): error (1)

Feature MPLS\_STATS (27): error (1)

Feature ETHERSTATS (28): error (1)

Feature CAPTURE (29): error (1)

Feature RMON1\_HOST (30): error (1)

Feature RMON1\_MATRIX (31): error (1)

Feature RMON2\_ADDRMAP (32): error (1)

Feature RMON2\_PDIST (33): error (1)

Feature RMON2\_HOST (34): error (1)

Feature RMON2\_MATRIX (35): error (1)

Feature DSMON\_STATS (36): error (1)

Feature DSMON\_PDIST (37): error (1)

Feature DSMON\_HOST (38): error (1)

Feature DSMON\_MATRIX (39): error (1)

Feature SMON\_PRIO (40): error (1)

Feature SMON\_VLAN (41): error (1)

# show debug messages

To display NAM log file contents, use the show debug messages command.

show debug messages

This command has no arguments or keywords.

This command has no default behavior or settings.

Command mode

The following example shows the log file contents:

root@nam.cisco.com# show debug messages

2008-10-14 00:07:11 \*\*\* FM Metric Engine 1 created (iThread 3)

2008-10-14 00:07:11 MAIN: Flow reaper starting, LWP = 1381

2008-10-14 00:07:11 Packet data and flow processing layers started successfully.

2008-10-14 00:07:11 WAAS: Load autoconfig: enables:1 client:1 cltwan:0 svrwan:0 server:0 passthru:0

2008-10-14 00:07:11 \*\*\* WAAS Flow Agent (FA) manager module initialized \*\*\*

2008-10-14 00:07:11 Load SA Export config SA\_EXPORT\_ENABLED = 0

2008-10-14 00:07:11 \*\*\* Configure SuperAgent export: export disabled

2008-10-14 00:07:11 \*\*\* ART Metric Engine post initialization done. \*\*\*

2008-10-14 00:07:11 MAIN: dbgport\_init: No cfg file!

2008-10-14 00:07:11 MAIN: Offtime LWP = 1382

2008-10-14 00:07:11 RPC: RPC LWP = 1383

2008-10-14 00:16:19 mond: exiting on signal 15.

2008-10-14 00:19:21 mond starting.

2008-10-14 00:19:21 MAIN: Timer LWP = 1570

2008-10-14 00:19:21 MAIN: Timekeeping LWP = 1571

# show debug metric-engine

To display metric-engine log file, use the show debug metric-enginecommand.

show debug metric-engine

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display metric-engine log file:

root@nam235Cat6k.cisco.com# show debug metric-engine

# show debug online-diag-stats

To display the online diagnostic status log file, use the show debug online-diag-statscommand.

show debug online-diag-stats

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the online diagnostic status log file:

root@nam235Cat6k.cisco.com# **show debug online-diag-stats**

Opcode/Subopcode RX TX Description

mgmt port 1 mgmt port 2 data port 1 data port 2

0 0 0 0

root@nam235Cat6k.cisco.com#

# show debug rise-messages

To display the debug RISE log messages, use the show debug rise-messagescommand. This command was introduced in NAM 6.0(1).

show debug rise-messages

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the debug RISE log messages:

root@nam.localdomain# show debug rise-messages

root@nam.localdomain#

# show decode-log

To display the packet decode log, use the show decode-log command. This command was introduced in 6.0(2).

show decode-log

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the packet decode log:

Root@localhost# show decode-log

Jan 17 23:47:51 nam NAM-PDS[4878]: Doing Startup

Jan 17 23:47:51 nam NAM-PDS[4878]: main: Basic pcap table generation to protocol typ

es and packet summmary information.

Jan 17 23:47:51 nam NAM-PDS[4878]: build\_capture\_file\_tables: The capture filename

is 'test1\_1.pcap'

Jan 17 23:47:51 nam NAM-PDS[4878]: tabularize\_capture\_file: Beginning tabularization

 for /storage/capture/test1\_1.pcap.

Jan 17 23:47:51 nam NAM-PDS[4878]: update\_table\_building\_status\_thread started

Jan 17 23:47:58 nam NAM-PDS[3911]: MSG: '{"txn\_id":0,"msg\_type":"request","opcode":"

get-packet-list","session-id":"analysis\_session\_1","pcap-file":"test1\_1.pcap","packe

t-numbers":"1-50","startPkt":"1","lastPkt":50,"count":"50","startPktNum":null,"sPktB

ound":null,"ePktBound":"48901","JSON":1}', rx 251

Jan 17 23:47:58 nam NAM-PDS[3911]: MSG: '{"txn\_id":0,"msg\_type":"request","opcode":"

fetch-packet-detail","session-id":"analysis\_session\_1","pcap-file":"test1\_1.pcap","p

ktnum":"1","JSON":1}', rx 147

Jan 17 23:48:01 nam NAM-PDS[4878]: update\_table\_building\_status\_thread finished

Jan 17 23:48:02 nam NAM-PDS[3911]: MSG: '{"txn\_id":0,"msg\_type":"request","opcode":"

get-capture-file-info","filename":"test1\_1.pcap","numOfPoints":200,"includeHistogram

":1}', rx 131

Jan 17 23:48:02 nam NAM-PDS[3911]: get\_packet\_summary\_header\_info: end of file for p

ktnum 50053 - Success

Jan 17 23:48:02 nam NAM-PDS[3911]: MSG: '{"txn\_id":0,"msg\_type":"request","opcode":"

get-packet-list","session-id":"analysis\_session\_1","pcap-file":"test1\_1.pcap","packe

t-numbers":"1-50","startPkt":"1","lastPkt":50,"count":"50","startPktNum":null,"sPktB

ound":null,"ePktBound":"50052","JSON":1}', rx 251

# show device

To display the remote devices like ERSPAN, NetFlow, and WAAS, use the show device command.

**show device**

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the remote devices:

root@localhost# show device

show email

To display email settings that are used for e-mailing alarm messages or scheduled reports, use the email command.

show email

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display email values:

root@localhost# show email

Email

 Server: example-email.domain.com

 Mail Alarm: enabled

 Alarm Recipients: admin@domain.com another\_admin@domain.com

root@localhost#

**device erspan**
**email**

# show entity

To display the serial number and the values of the entity MIB entPhysicalAlias and entPhysicalAssetID, use the show entity command.

show entity

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display entity values:

root@localhost# show entity

Serial Number : SAD061506JU

Alias :

Asset ID :

**entity alias**

**entity assetid**

# show ftp

To display the FTP server and directory for storing scheduled reports configuration, use the show ftp command.

show ftp

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the FTP server configuration:

root@localhost# show ftp

FTP settings:

 Server: my.ftp-server.com

 Directory: /my/directory

 User: myUserName

# show hosts

To display the hosts entries, use the show hosts command.

show hosts

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the hosts entries:

Root@localhost# show hosts

# $Id: hosts,v 1.5 2003/08/07 01:47:51 pwildi Exp $

#

127.0.0.1 localhost localhost.localdomain

10.10.10.2 trifecta-p2c-30.cisco.com trifecta-p2c-30

1.1.1.1 trifecta-p2c-30.cisco.com trifecta-p2c-30

10.0.0.0 trifecta-p2c-30.cisco.com trifecta-p2c-30

# show interface management-port

To display the configuration and statistics of management interface, use the show interface management-port command. This command was introduced in NAM 6.0(1).

show interface management-port

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the configuration and statistics of management interface:

root@nam.localdomain# show interface management-port

eth0 Link encap:Ethernet HWaddr 50:3D:E5:9E:33:06

 inet addr:172.20.122.196 Bcast:172.20.122.255 Mask:255.255.255.128

 inet6 addr: fe80::523d:e5ff:fe9e:3306/64 Scope:Link

 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

 RX packets:892882 errors:0 dropped:0 overruns:0 frame:0

 TX packets:432497 errors:0 dropped:0 overruns:0 carrier:0

 collisions:0 txqueuelen:1000

 RX bytes:165147017 (157.4 MiB) TX bytes:77233177 (73.6 MiB)

 Memory:dfa00000-dfb00000

root@nam.localdomain#

# show internal resources monitoring

To display the resources used for monitor features, use the show internal resources monitoring command. This command was introduced in NAM 6.0(2).

show internal resources monitoring

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the resources used for monitor features:

root@nam.localdomain# show internal resources monitoring

Regular FM threads : 3

Non-promiscuous FM threads : 1

TCP flows per FM : 1000000

TCP flows for NP : 2500000

TCP flows total : 5500000 (2368 bytes each)

UDP flows per FM : 1000000

UDP flows for NP : 1000000

UDP flows total : 4000000 (1024 bytes each)

SCTP flows per FM : 10000

SCTP flows for NP : 50000

SCTP flows total : 80000 (1024 bytes each)

IP flows per FM : 100000

IP flows for NP : 250000

IP flows total : 550000 (896 bytes each)

L2 flows per FM : 50000

L2 flows for NP : 50000

L2 flows total : 200000 (768 bytes each)

Total flows : 10330000

URL entries per FM : 10000

URL entries for NP : 50000

URL entries total : 80000 (552 bytes each)

Sensor threads : 3

RTP streams per thread : 60000

Total RTP streams : 180000 (160 bytes each)

Conversation Records : 600000 (192 bytes each)

Conversation Records (PA) : 100000

Host Records : 300000 (152 bytes each)

Site Records : 40000 (152 bytes each)

Site Matrix Records : 80000 (52 bytes each)

Data Source Records : 30000 (116 bytes each)

ART Records : 600000 (428 bytes each)

ART Records (PA) : 100000

ART Server Records : 100000 (316 bytes each)

ART Client Records : 200000 (316 bytes each)

RTP stream records : 20000 (164 bytes each)

RTP MOS records : 4000 (28 bytes each)

Voice records : 10000 (672 bytes each)

root@nam.localdomain#

# show inventory

To display the system inventory information for a NAM device, use the show inventory command.

show inventory

This command has no arguments or keywords.

No default behavior or values.

Command mode

The show inventory command allows you to view the UDI for a NAM device. This identity information is stored in the NAM device’s non-volatile memory.

* PID—Product identification (ID) number of the device
* VID—Version ID of the device. Displays as 0 if the version number is not available.
* SN—Serial number of the device

The following example shows the system inventory information:

root@nam.cisco.com# show inventory

PID:WS-SVC-NAM-3-K9 VID:v01 SN:SAL1444YBFU

# show ip

To display the NAM IP parameters, use the show ip command.

show ip

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM IP parameters:

Root@localhost# show ip

IP address: 101.10.11.189

Subnet mask: 255.255.255.255

IP Broadcast: 111.20.255.255

DNS Name: namlab-kom9.cisco.com

Default Gateway: 111.20.98.125

Nameserver(s): 111.69.2.135

HTTP server: Enabled

HTTP secure server: Disabled

HTTP port: 80

HTTP secure port: 443

TACACS+ configured: No

Telnet: Enabled

SSH: Disabled

**ip address**

**ip broadcast**

**ip gateway**

**ip host**

**ip hosts add**

**ip hosts delete**

**ip http secure generate**

**ip http secure port**

**ip http secure server**

**ip http tacacs+**

# show license

To display the information about the license installed on the WAE device.

show license

* This command is not valid for NAM-1, NAM-2, NME-NAM-80S, NME-NAM-120S, or the Cisco NAM 2200 Series appliances.

This command has no arguments or keywords.

This command has no default settings.

Command mode

This command is valid only on the NAM Virtual Blade.

This example shows how to display the NAM Virtual Blade license information for the WAE device.

Root@localhost# show license

**license install**

**config upload**

# show local-storage all

To show all physical disks and virtual drives, use the show local-storage all command.

show local-storage all

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display all physical disks and virtual drives:

Root@localhost# show local-storage all

==============================================================================
Adapter: 0
Product Name: LSI MegaRAID SAS 9266-8i
Memory: 1024MB
BBU: Present
Serial No:
==============================================================================

Number of DISK GROUPS: 2
DISK GROUP: 0

Number of Spans: 1

SPAN: 0

Span Reference: 0x00

Number of PDs: 2

Number of VDs: 1

Number of dedicated Hotspares: 0

Virtual Drive Information:

Virtual Drive: 0 (Target Id: 0)

Name                :

RAID Level          : Primary-1, Secondary-0, RAID Level Qualifier-0

Size                : 930.390 GB

State               : Optimal

Strip Size          : 64 KB

Number Of Drives    : 2

Span Depth          : 1

Default Cache Policy: WriteThrough, ReadAheadNone, Direct, No Write Cache if Bad BBU

Current Cache Policy: WriteThrough, ReadAheadNone, Direct, No Write Cache if Bad BBU

Access Policy       : Read/Write

Disk Cache Policy   : Disk's Default

Encryption Type     : None

Physical Disk Information:

Physical Disk: 0

Enclosure Device ID: 64

Slot Number: 0

Enclosure position: 0

Device Id: 0

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221100000000

Connected Port Number: 0(path0)

Inquiry Data:             9XG0ZWCHST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

Physical Disk: 1

Enclosure Device ID: 64

Slot Number: 1

Enclosure position: 0

Device Id: 3

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221101000000

Connected Port Number: 1(path0)

Inquiry Data:             9XG101Y4ST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

DISK GROUP: 1

Number of Spans: 1

SPAN: 0

Span Reference: 0x01

Number of PDs: 6

Number of VDs: 1

Number of dedicated Hotspares: 0

Virtual Drive Information:

Virtual Drive: 0 (Target Id: 1)

Name                :

RAID Level          : Primary-5, Secondary-0, RAID Level Qualifier-3

Size                : 4.541 TB

State               : Optimal

Strip Size          : 64 KB

Number Of Drives    : 6

Span Depth          : 1

Default Cache Policy: WriteThrough, ReadAhead, Direct, No Write Cache if Bad BBU

Current Cache Policy: WriteThrough, ReadAheadNone, Direct, No Write Cache if Bad BBU

Access Policy       : Read/Write

Disk Cache Policy   : Disk's Default

Encryption Type     : None

Physical Disk Information:

Physical Disk: 0

Enclosure Device ID: 64

Slot Number: 7

Enclosure position: 0

Device Id: 7

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221107000000

Connected Port Number: 7(path0)

Inquiry Data:             9XG1032BST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :32 Celsius

Physical Disk: 1

Enclosure Device ID: 64

Slot Number: 5

Enclosure position: 0

Device Id: 6

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221105000000

Connected Port Number: 5(path0)

Inquiry Data:             9XG10211ST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :31 Celsius

Physical Disk: 2

Enclosure Device ID: 64

Slot Number: 6

Enclosure position: 0

Device Id: 5

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221106000000

Connected Port Number: 6(path0)

Inquiry Data:             9XG102TSST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :31 Celsius

Physical Disk: 3

Enclosure Device ID: 64

Slot Number: 4

Enclosure position: 0

Device Id: 4

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221104000000

Connected Port Number: 4(path0)

Inquiry Data:             9XG0ZTCRST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

Physical Disk: 4

Enclosure Device ID: 64

Slot Number: 2

Enclosure position: 0

Device Id: 2

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221102000000

Connected Port Number: 3(path0)

Inquiry Data:             9XG102M3ST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :31 Celsius

Physical Disk: 5

Enclosure Device ID: 64

Slot Number: 3

Enclosure position: 0

Device Id: 1

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221103000000

Connected Port Number: 2(path0)

Inquiry Data:             9XG10CNKST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

**show local-storage physical**

**show local-storage progress**

**show local-storage virtual**

# show local-storage physical

To show physical drive information for local disks, use the show local-storage physcial command.

show local-storage physical

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the maintenance image import log entries:

Root@localhost# show local-storage physical

Adapter #0

Enclosure Device ID: 64

Slot Number: 0

Enclosure position: 0

Device Id: 0

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221100000000

Connected Port Number: 0(path0)

Inquiry Data:             9XG0ZWCHST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

Enclosure Device ID: 64

Slot Number: 1

Enclosure position: 0

Device Id: 3

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221101000000

Connected Port Number: 1(path0)

Inquiry Data:             9XG101Y4ST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

Enclosure Device ID: 64

Slot Number: 2

Enclosure position: 0

Device Id: 2

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221102000000

Connected Port Number: 3(path0)

Inquiry Data:             9XG102M3ST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :31 Celsius

Enclosure Device ID: 64

Slot Number: 3

Enclosure position: 0

Device Id: 1

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221103000000

Connected Port Number: 2(path0)

Inquiry Data:             9XG10CNKST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

Enclosure Device ID: 64

Slot Number: 4

Enclosure position: 0

Device Id: 4

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221104000000

Connected Port Number: 4(path0)

Inquiry Data:             9XG0ZTCRST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :30 Celsius

Enclosure Device ID: 64

Slot Number: 5

Enclosure position: 0

Device Id: 6

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221105000000

Connected Port Number: 5(path0)

Inquiry Data:             9XG10211ST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :31 Celsius

Enclosure Device ID: 64

Slot Number: 6

Enclosure position: 0

Device Id: 5

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221106000000

Connected Port Number: 6(path0)

Inquiry Data:             9XG102TSST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :31 Celsius

Enclosure Device ID: 64

Slot Number: 7

Enclosure position: 0

Device Id: 7

Sequence Number: 2

Media Error Count: 0

Other Error Count: 0

Predictive Failure Count: 0

Last Predictive Failure Event Seq Number: 0

PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]

Non Coerced Size: 931.012 GB [0x74606db0 Sectors]

Coerced Size: 930.390 GB [0x744c8000 Sectors]

Firmware state: Online, Spun Up

SAS Address(0): 0x4433221107000000

Connected Port Number: 7(path0)

Inquiry Data:             9XG1032BST91000640NS                            CC02

FDE Capable: Not Capable

FDE Enable: Disable

Secured: Unsecured

Locked: Unlocked

Needs EKM Attention: No

Foreign State: None

Device Speed: 6.0Gb/s

Link Speed: 6.0Gb/s

Media Type: Hard Disk Device

Drive:  Not Certified

Drive Temperature :32 Celsius

**show local-storage all**

**show local-storage progress**

**show local-storage virtual**

# show local-storage progress

To show RAID array construction or deconstruction progress for local disks, use the show local-storage progress command.

show local-storage progress

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display RAID array construction or deconstruction progress for local disks:

Root@localhost# show local-storage progress

Individual Disk Rebuild

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

Device(Encl-64 Slot-0) is not in rebuild process
Device(Encl-64 Slot-1) is not in rebuild process

Device(Encl-64 Slot-2) is not in rebuild process

Device(Encl-64 Slot-3) is not in rebuild process

Device(Encl-64 Slot-4) is not in rebuild process

Device(Encl-64 Slot-5) is not in rebuild process

Device(Encl-64 Slot-6) is not in rebuild process

Device(Encl-64 Slot-7) is not in rebuild process

Exit Code: 0x00

Virtual Drive Reconstruction

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

Reconstruction on VD #0 is not in Progress.

Exit Code: 0x00

Reconstruction on VD #1 is not in Progress.

Exit Code: 0x00

**show local-storage all**

**show local-storage progress**

**show local-storage virtual**

# show local-storage virtual

To how to display virtual drive (RAID array) information for local disks, use the show local-storage virtual command.

show local-storage virtual

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display virtual drive (RAID array) information for local disks:

Root@localhost# show local-storage virtual

Adapter 0 -- Virtual Drive Information:

Virtual Drive: 0 (Target Id: 0)

Name                :

RAID Level          : Primary-1, Secondary-0, RAID Level Qualifier-0

Size                : 930.390 GB

State               : Optimal

Strip Size          : 64 KB

Number Of Drives    : 2

Span Depth          : 1

Default Cache Policy: WriteThrough, ReadAheadNone, Direct, No Write Cache if Bad BBU

Current Cache Policy: WriteThrough, ReadAheadNone, Direct, No Write Cache if Bad BBU

Access Policy       : Read/Write

Disk Cache Policy   : Disk's Default

Encryption Type     : None

Virtual Drive: 1 (Target Id: 1)

Name                :

RAID Level          : Primary-5, Secondary-0, RAID Level Qualifier-3

Size                : 4.541 TB

State               : Optimal

Strip Size          : 64 KB

Number Of Drives    : 6

Span Depth          : 1

Default Cache Policy: WriteThrough, ReadAhead, Direct, No Write Cache if Bad BBU

Current Cache Policy: WriteThrough, ReadAheadNone, Direct, No Write Cache if Bad BBU

Access Policy       : Read/Write

Disk Cache Policy   : Disk's Default

Encryption Type     : None

Exit Code: 0x00

**show local-storage all**

**show local-storage physical**

**show local-storage progress**

# show log config

To display the maintenance image configuration import log entries, use the show log config command.

show log config

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the maintenance image import log entries:

Root@localhost# show log config

**config clear**

**show log report**

**upgrade**

# show log patch

To display the patch log entries, use the show log patch command.

show log patch

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the maintenance image import log entries:

Root@localhost# show log patch

**config clear**

**show log report**

**upgrade**

# show log report

To display the import log entries, use the show log report command.

show log report

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the import log entries:

Root@localhost# show log report

**show log config**

# show log upgrade

To display the maintenance image upgrade log entries, use the show log upgrade command.

show log upgrade

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the maintenance image upgrade entries:

Root@localhost# show log upgrade

Fri Aug 23 10:32:27 2002 : path: ftp://namlab-pc1/pub/rmon/MP-KPLUS

 Fri Aug 23 10:32:27 2002 : file: mp-dev.1-2-0-5.bin

 Fri Aug 23 10:32:27 2002 : extn: .gz

 Fri Aug 23 10:32:27 2002 : Downloading the image...

 Fri Aug 23 10:32:28 2002 : Successfully downloaded the image...

 Fri Aug 23 10:32:28 2002 : Uncompressing the image...

 Fri Aug 23 10:32:29 2002 : Finished uncompressing the file /tmp/mp-dev.1-2-0-5. bin.gz.

 Fri Aug 23 10:32:29 2002 : Successfully uncompressed the image.

 Fri Aug 23 10:32:29 2002 : Verifying the image...

 Fri Aug 23 10:32:29 2002 : opening file /tmp/mp-dev.1-2-0-5.bin.ver

 Fri Aug 23 10:32:30 2002 : Successfully verified the image.

 Fri Aug 23 10:32:30 2002 : Partition '/dev/hda1' unmounted.

 Fri Aug 23 10:32:30 2002 : Applying the Maintenance image.

 Fri Aug 23 10:32:30 2002 : This process may take several minutes...

 Fri Aug 23 10:32:30 2002 : Writing mbr...

 Fri Aug 23 10:32:30 2002 : Successfully wrote mbr.

 Fri Aug 23 10:32:30 2002 : Number of Sectors: 31

 Fri Aug 23 10:32:30 2002 : Writing grub and maint image.

 Fri Aug 23 10:33:18 2002 : Successfully wrote the maint image.

 Fri Aug 23 10:33:18 2002 : Partition '/dev/hda1' mounted.

 Fri Aug 23 10:33:18 2002 : Performing post install...

 Fri Aug 23 10:33:18 2002 : File /usr/local/nam/falcon\_version copied to /mnt/mp /boot/appl/daughter\_card.info.

 Fri Aug 23 10:33:18 2002 : Maintenance image upgrade completed successfully.

**upgrade**

# show memory

To display the installed memory, available memory, and the memory being used by the system, use the show memory command.

show memory

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM memory:

Root@localhost# show memory

Installed: 858 MB

Available: 240 MB

System Usage: 617 MB

**show cdb**

# show metric export

To show metric export configuration, use the show metric export command.

show metric export

This command has no arguments or keywords.

No default behavior or values.

Command mode

The following example shows the metric export configuration:

root@nam.cisco.com# show metric export

Metric export: enabled

Host: 10.0.0.1

Port: 9995

Export non-WAAS traffic: enabled

# show monitor protocol encapsulation

To display the encapsulation configurations, use the **show** **monitor protocol encapsulation** command. This command is removed in NAM 6.0(1)

show monitor protocol encapsulation

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the encapsulation configurations:

root@nam.cisco.com# show monitor protocol encapsulation

**monitor protocol encapsulation**

# show monitor protocol all

To display all of the protocols in the protocol directory, use the show monitor protocol all command. This command is removed in NAM 6.0(1).

show monitor protocol all

This command has no arguments or keywords.

This command has no default settings.

Command mode

This command is supported on all NAM platforms.

This example shows how to display all of the protocol configurations:

Root@localhost# show monitor protocol all

Control Index: 46232

Data Source: dataport1

Owner: LocalMgr

Status: 1

Root@localhost#

# show monitor rtp-stream

To display the RTP monitoring and alarm threshold settings, use the show monitor rtp-stream command.

show monitor rtp-stream

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the RTP-stream monitoring settings and alarm thresholds.

root@localhost# show monitor rtp-stream

root@localhost#

**monitor rtp-stream enable**

**monitor urlcollection**

show monitor rtp-stream filter

To display the URL collection configuration, use the **show** **monitor** rtp-stream filter command.

show monitor rtp-stream filter

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the URL collection statistics:

root@localhost# show monitor rtp-stream filter

root@localhost#

**monitor rtp-stream filter**

# show monitor urlcollection

To display the URL collection configuration, use the show monitor urlcollection command.

show monitor urlcollection

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the URL collection statistics:

root@localhost# show monitor urlcollection

root@localhost#

**monitor urlcollection**

# show monitor urlfilter

To display the URL filter configuration, use the show monitor urlfilter command. This command is removed in NAM 6.0(1).

show monitor urlfilter [control-index]

|  |  |
| --- | --- |
| control-index | (Optional) Specifies the URL filter control index. |

This command has no default settings.

Command mode

This example shows how to display the URL filter configuration:

root@localhost# show monitor urlfilter

root@localhost#

**monitor urlfilter**

# 6: NAM CLI Commands: show password strong-policy - web user\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This chapter describes the following NAM CLI commands:

* [show password strong-policy](#_Toc330562059)
* [show patches](#_Toc330562060)
* [show pkt-drop counters](#_Toc330562061)
* [show preferences](#_Toc330562062)
* [show protocol-feature](#_Toc330562063)
* [show remote-storage](#_Toc330562064)
* [show rxcounters](#_Toc330562065)
* [show snmp](#_Toc330562066)
* [show syslog-settings](#_Toc330562067)
* [show system-alerts](#_Toc330562068)
* [show tech-support](#_Toc330562069)
* [show time](#_Toc330562070)
* [show time ptp](#_Toc330562071)
* [show trap-dest](#_Toc330562072)
* [show version](#_Toc330562073)
* [show waas data-source](#_Toc330562074)
* [show waas device](#_Toc330562075)
* [show waas server filter](#_Toc330562076)
* [show web-publication](#_Toc330562077)
* [show web-user](#_Toc330562078)
* [shutdown](#_Toc330562079)
* [snmp](#_Toc330562080)
* [syslog](#_Toc330562081)
* [syslog remote-server](#_Toc330562082)
* [terminal](#_Toc330562083)
* [time](#_Toc330562084)
* [traceroute](#_Toc330562085)
* [trap-dest](#_Toc330562086)
* [upgrade](#_Toc330562087)
* [waas export server-filter-list](#_Toc330562088)
* [waas import server-filter-list](#_Toc330562089)
* [waas server filter](#_Toc330562090)
* [web-publication](#_Toc330562091)
* [web-user](#_Toc330562092)

# show password strong-policy

To display the strong password policy settings for user names, use the show password strong-policy command.

show password strong-policy

This command has no default settings.

Command mode

There is only one valid user, root. (as of NAM 6.X)

This example shows how to set a password:

root@localhost.cisco.com# show password strong-policy

Strong password policy is enabled.

# show patches

To display all of the installed patches, use the show patches command.

show patches

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display all of the installed patches:

Root@localhost# show patches

**patch**

# show pkt-drop counters

To display the NAM hardware, flow manager, and the metrics engine drop, use the show pkt-drop counters command.

show pkt-drop counters

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM hardware, flow manager, and the metrics engine drop:

Root@localhost# **show pkt-drop-counters**

Hour-0 - show the current hour pkts drop counter

Hour-1 - show the last hour pkts drop counter

Hour-10 - show the last 10th hour pkts drop counter

Hour-11 - show the last 11th hour pkts drop counter

Hour-12 - show the last 12th hour pkts drop counter

Hour-13 - show the last 13th hour pkts drop counter

Hour-14 - show the last 14th hour pkts drop counter

Hour-15 - show the last 15th hour pkts drop counter

Hour-16 - show the last 16th hour pkts drop counter

Hour-17 - show the last 17th hour pkts drop counter

Hour-18 - show the last 18th hour pkts drop counter

Hour-19 - show the last 19th hour pkts drop counter

Hour-2 - show the last 2nd hour pkts drop counter

Hour-20 - show the last 20th hour pkts drop counter

Hour-21 - show the last 21st hour pkts drop counter

Hour-22 - show the last 22nd hour pkts drop counter

Hour-23 - show the last 23rd hour pkts drop counter

Hour-3 - show the last 3rd hour pkts drop counter

Hour-4 - show the last 4th hour pkts drop counter

Hour-5 - show the last 5th hour pkts drop counter

Hour-6 - show the last 6th hour pkts drop counter

Hour-7 - show the last 7th hour pkts drop counter

Hour-8 - show the last 8th hour pkts drop counter

Hour-9 - show the last 9th hour pkts drop counter

# show preferences

To display the configured preferences for your screen, use the show preferences command.

show preferences

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the configured screen preferences:

root@localhost.cisco.com# show preferences

Entries per screen: 15

Refresh interval: 60 secs

Number of graph bars: 10

Hostname resolution: Disabled

Data displayed in: Bytes

Format large number: No

Number notation: Commas-dot

root@localhost.cisco.com#

**preferences**

# show protocol-feature

To display the parsing protocol feature, use the **show protocol-feature** command.

show protocol-feature

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the parsing protocol feature:

root@NAM.cisco.com# **show protocol-feature**

# show remote-storage

To display the network storage target for report and capture date, use the show remote-storage command.

 **show remote-storage**

This command has no keywords or arguments.

This command has no default settings.

Command mode

This example shows how to display the web user information:

root@localhost.cisco.com# show remote-storage

# show rxcounters

To display the number of packets received by NAM data ports, use the show rxcounters command.

show rxcounters

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the number of packets received by NAM data ports:

root@nam235Cat6k.cisco.com# show rxcounters

data port 1 rx pkt count: 193327281

data port 2 rx pkt count: 1164

root@nam235Cat6k.cisco.com#

# show snmp

To display the SNMP parameters, use the show snmp command.

show snmp

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the SNMP parameters:

Root@localhost# show snmp

SNMP Agent: mynam.cisco.com 209.265.200.225

SNMPv1: Enabled

SNMPv2C: Enabled

SNMPv3: Disabled

community private write

community public read

trap community public 112.10.17.237

trap community public 112.10.17.244

sysDescr Cisco Catalyst 6500 Series Network Analysis Module (WS-SVC-NAM-3-K9) Console, 5.0(1T.45)

Copyright (c) 1999-2011 by Cisco Systems, Inc.

sysObjectID workgroup.1.3.1.1.2.291

sysContact engineer

sysName mynam

sysLocation RMON Lab

**snmp**

# show syslog-setting**s**

To display the NAM system log settings, use the show syslog-settings command.

show syslog-settings

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM system log settings:

root@localhost# **show syslog-settings**

Remote server 1: 172.20.98.177

Remote server 2: 10.0.0.12

root@localhost#

**syslog**

# show system-alerts

To display NAM failures or problems, use the show system-alerts command.

show system-alerts

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM system alerts:

Root@localhost# show system-alerts

Jan 1 15:07:31 mynam scpd: scpd: 0x10/44 -> 0x15/0, len 18, op 0x14a, len

 2, flags 0(), seq 65443, ver 0

Jan 1 15:07:31 mynam scpd: scpd: SCP PC Blade REQ from 0x10/44.

Jan 1 15:07:31 mynam scpd: scpd: sub-opcode 6, status 45.

Jan 1 15:07:31 mynam scpd: scpd: SCP PC Shutdown.

Jan 1 15:07:33 mynam scpd: scpd: shutdown of NAM!

Jan 1 15:07:35 mynam rmond[595]: rmond: received QUIT signal! Exiting!

Jan 1 15:07:38 mynam polld: Terminating polld.

Jan 1 15:07:42 mynam configd: SIGTERM recieved.

Jan 1 15:07:42 mynam configd: Terminating with success.

Jan 1 00:02:43 mynam scpd: scpd: 0x10/1 -> 0x15/0, len 18, op 0x14a, len

# show tech-support

To display technical support information, use the show tech-support command.

show tech-support

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM technical support information:

Root@localhost# show tech-support

PID TTY STAT TIME COMMAND

 1 ? S 0:08 init

 2 ? SW 0:00 [keventd]

 3 ? SWN 0:00 [ksoftirqd\_CPU0]

 4 ? SWN 0:00 [ksoftirqd\_CPU1]

 5 ? SW 0:00 [kswapd]

 6 ? SW 0:00 [bdflush]

 7 ? SW 0:05 [kupdated]

 238 ? S 0:00 /usr/local/nam/bin/scpd -l -d/var/log/scpd

 246 ? SW 0:10 [kjournald]

 474 ? S 0:01 syslogd -m 0

 477 ? S 0:00 klogd -2

 501 ? S 0:00 /usr/sbin/atd

# show time

To display NAM time zone or time synchronization settings, use the show time command.

show time

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to display the NAM time settings:

Root@localhost# show time

NAM synchronize time to: Switch

Timezone configured on the switch: PDT

Current system time: Thu May 1 09:29:49 GMT+8 2003

**time**

# show time ptp

To display PTP specific time settings, use the show time ptp command. This command is removed in NAM 6.0(1).

show time ptp

This command has no arguments or keywords.

This command has no default settings.

Command mode

When you enter the command, the following commands are available:

* **clock**—Displays PTP clock information.
* **foreign-master-record**—Displays PTP foreign master records.
* **parent -** Displays PTP parent properties.
* **time-property -** Displays PTP clock time property.

This example shows how to display the time settings:

Root@localhost# show time ptp

clock - show ptp clock information

foreign-master-record - show ptp foreign master records

parent - show ptp parent properties

time-property - show ptp clock time property

# show trap-dest

To display all of the NAM trap destinations, use the show trap-dest command.

show trap-dest [trap-index]

|  |  |
| --- | --- |
| trap-index | (Optional) Displays the trap destinations by the specified trap index. |

This command has no default settings.

Command mode

This example shows how to display the NAM trap destinations:

Root@localhost# show trap-dest

Trap index: 23370

Community: public

Address: 172.20.98.136

UDP port: 162 (00a2)

Owner: LocalMgr

Root@localhost#

**traceroute6**

To trace the route to a IPv6 network device, use the traceroute6 command. This command was introduced in NAM 6.0(1).

traceroute [ n | v] [-m max\_ttl] [-p port] [-s src\_addr] [-w waittime] destination host name | IPv6 address

|  |  |
| --- | --- |
| **-n** | (Optional) Prints hop addresses numerically. |
| **-v** | (Optional) Sets the output to verbose. |
| **-m max\_ttl** | (Optional) Sets the maximum time-to-live (max number of hops) used. |
| **-p port** | (Optional) Sets the base UDP port number used in probes. |
| **-s src\_addr** | (Optional) Forces the source address to be an address other than the IP address of the interface the packet is sent on. |
| **-w waittime** | (Optional) Sets the time (in seconds) to wait for a response to a probe. |

This command has no default settings.

Command mode

This example shows how to trace a route to a network device named aragon:

trap-dest

# show top-memory-users

To display the NAM top memory users, use the show top-memory-users command. This command was introduced in NAM 6.0(1).

 **show top-memory-users**

This command has no keywords or arguments.

This command has no default settings.

Command mode

This example shows how to display the NAM top memory users:

root@nam.localdomain# show top-memory-users

Top memory usage information not available.

root@nam.localdomain#

# show version

To display the NAM version information, use the show version command.

 **show version**

This command has no keywords or arguments.

This command has no default settings.

Command mode

This example shows how to display the NAM version information:

Root@localhost# show version

NAM application image version: 5.0(1T.45) INTERIM SOFTWARE

Helper Version: 1.1(0.19)

Gold Helper Version: 1.1(0.19)

PID: WS-SVC-NAM-3-K9

Memory size: 23 GB

Disk 0 size: 8 GB

Disk 1 size: 600 GB

Installed patches:

No patches are installed on this system.

Root@localhost#

**config clear**

# show waas data-source

To display the WAAS devices configured on the NAM device, use the show waas data-source command.

show waas data-source [datasrc-index]

|  |  |
| --- | --- |
| datasrc-index | (Optional) Displays the data source index |

The default behavior is to show all WAAS data sources unless a specific data source index is specified.

Command mode

This command is supported on all NAM platforms.

The show waas data-source command displays information about WAAS data sources currently configured on the NAM.

The following example shows the system inventory information:

root@nam.cisco.com# show waas data-source

root@nam.cisco.com#

# show waas device

To display the WAAS devices configured on the NAM device, use the show waas device command.

show waas device [ip-address]

|  |  |
| --- | --- |
| ip-address | IP address of the WAAS device (optional) |

The default behavior is to show all WAAS devices unless IP address is specified.

Command mode

This command is supported on all NAM platforms.

The following example shows the system inventory information:

root@nam.cisco.com# show waas device

root@nam.cisco.com#

# show waas server filter

To show WAAS server filter list, use the show waas server filter command.

show waas server filter

This command has no arguments or keywords.

This command has no default settings.

Command mode

The following example shows how to display the waas server filters.

root@nam.cisco.com# show waas server filter

10.0.0.2

# show web-publication

To display the web publication hosts configuration information, use the show web-publication command.

 **show web-publication**

This command has no keywords or arguments.

This command has no default settings.

Command mode

This example shows how to display the web user information:

Root@localhost# show web-publication

Web publication: enabled

Allowed hosts:

Access code:

Alarm screens: disabled

Report screens: enabled

Voice screens: enabled

RMON screens: enabled

**web-publication**

# show web-user

To display the web user information, use the show web-user command.

 **show web-user** [username]

|  |  |
| --- | --- |
| username | (Optional) Displays the specified user name information. |

This command has no default settings.

Command mode

This example shows how to display the web user information:

Root@localhost# show web-user admin

User: admin

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

Account management: Enabled

System config: Enabled

Capture: Enabled

Alarm config: Enabled

Collection config: Enabled

Collection view: Enabled

Console

**web-user**

# shutdown

To shut down the NAM, use the shutdown command.

shutdown

This command has no arguments or keywords.

This command has no default settings.

Command mode

This example shows how to shut down the NAM:

Root@localhost# shutdown

Shut down the NAM? (y/n) [n]: n

**exit**

**logout**

**preferences**

# snmp

To configure NAM system MIB objects, use the snmp command.

snmp communit**y** community-string { ro | rw }

snmp delete community community-string

snmp contact contact-string

snmp location location-string

snmp name name-string

|  |  |
| --- | --- |
| **community** community-string ro | rw | Sets the device community string. |
| **delete** community-string | Deletes the device community string. |
| **contact** contact-string | Sets the device contact string. |
| **location** location-string | Sets the device location. |
| **name** name-string | Sets the device name. |

This command has no default settings.

Command mode

This example shows how to configure NAM system MIB objects:

Root@localhost# snmp community askdfhtjlks.01‘ contact george location frisco, name al

**show snmp**

# syslog

To enter the system log subcommand mode, and then configure system logging for the NAM, use the syslog command.

syslog

This command has no arguments or keywords.

This command has no default settings.

Command mode

When you enter the system log subcommand mode, the following commands are available:

* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **help** - Displays help
* **remote-server**—(Optional) Configures the system log for remote logging.

This example shows how to configure system logging for the NAM:

Root@localhost# syslog

root@localhost.cisco.com(sub-syslog)#

**show syslog-setting**s

# syslog remote-server

To capture NAM remote server alarms, use the remote-server subcommand from the syslog subcommand mode.

remote-server **disable** | [**server1** [**server2**] [**server3**] [**server4**] [**server5**]

|  |  |
| --- | --- |
| disable | Disables remote server event logging. |
| server1 server2 server3 server4 server5 | (Optional) Specifies the remote server. |

This command has no default settings.

Syslog subcommand mode

This command is supported on all NAM platforms.

This example shows how to configure the NAM to capture remote server alarms:

root@localhost# **syslog**

Entering into subcommand mode for this command.

Type 'exit' to apply changes and come out of this mode.

Type 'cancel' to discard changes and come out of this mode.

root@localhost(sub-syslog)# **remote-server 10.0.0.7 10.0.0.40**

root@localhost(sub-syslog)# exit

NAM syslog settings updated successfully..

**audit-trail enable**

**show syslog-setting**s

**syslog**

**web-user**

# terminal

To set the number of lines on a screen for this session, use the terminal command.

terminal editor [enable | **d**isable]

terminal length length

terminal mode { 0 | 1}

|  |  |
| --- | --- |
| **editor** [**enable** | d**isable**] | (Optional) Enables or disables the NAM CLI command editing. |
| **length** length | Sets the number of lines per screen for a session. |
| **mode** { **0** | **1**} | Sets the terminal mode. |

This command has no default settings.

Command mode

This example shows how to set the number of lines on a session’s screen:

root@localhost# terminal length 24

Terminal length for this session set to 24.

**config clear**

# time

To enter the time configuration subcommand mode, and then configure NAM system time settings, use the time command.

time

This command has no arguments or keywords.

This command has no default settings.

Switch command

Privileged

When you enter the time configuration subcommand mode, the following commands are available:

* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **sync ntp | switch**—(Optional) Synchronizes the NAM system time with the Network Time Protocol (NTP) or with the switch.
* zone—region-name [zone-name]—Synchronizes the time zone with the NAM for use with NTP.
* ptp-ip-address—Sets the ip address of the ptp interface.

This example shows how to configure system time settings on the NAM to synchronizes the time with the switch:

root@hostname.cisco.com# time

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@hostname.cisco.com(sub-time)# ?

? - display help

cancel - discard changes and exit from subcommand mode

exit - exit from subcommand mode

help - display help

ptp-ip-address - set the ip address of the ptp interface

sync - synchronize NAM system time with switch or ntp

root@hostname.cisco.com(sub-time)# sync switch

root@hostname.cisco.com(sub-time)# exit

Successfully updated NAM system time settings.

NOTE:You have configured the NAM synchronize time to the switch.

For this change to take effect, set the time from the switch or

reset the NAM.

root@hostname.cisco.com# show time

NAM synchronize time to: Switch

Timezone configured on the switch:PST

Switch time offset to UTC: 0

Current system time: Thu Mar 20 09:23:14 GMT 2003

This example shows how to configure system time settings on the NAM to synchronize the time with the NTP:

root@hostname.cisco.com# time

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@hostname.cisco.com(sub-time)# sync ntp ntp01.cisco.com ntp02.cisco.com

root@hostname.cisco.com(sub-time)# exit

Successfully updated NAM system time settings.

root@hostname.cisco.com# show time

NAM synchronize time to: NTP

NTP server1: ntp01.cisco.com

NTP server2: ntp02.cisco.com

Current system time: Thu Mar 20 09:23:36 GMT 2003

root@hostname.cisco.com#

**show time**

# traceroute

To trace the route to a IPv4 network device, use the traceroute command.

traceroute [-I | n | v] [-f first\_ttl] [-m max\_ttl] [-p port] [-s src\_addr] [-t tos] [-w waittime] destination host name | IP address [packetlen]

|  |  |
| --- | --- |
| **-I** | (Optional) Specifies that ICMP ECHO is used instead of UDP datagrams. |
| **-n** | (Optional) Prints hop addresses numerically. |
| **-v** | (Optional) Sets the output to verbose. |
| **-f first\_ttl** | (Optional) Sets the initial time-to-live used in the first outgoing packet. |
| **-m max\_ttl** | (Optional) Sets the maximum time-to-live (max number of hops) used. |
| **-p port** | (Optional) Sets the base UDP port number used in probes. |
| **-s src\_addr** | (Optional) Forces the source address to be an address other than the IP address of the interface the packet is sent on. |
| **-t tos** | (Optional) Sets the type-of-service in packets to the following value. |
| **-w waittime** | (Optional) Sets the time (in seconds) to wait for a response to a probe. |
| **destination** | Sets the packet destination. |
| **host** | Sets the host. |
| **name** | Sets the hostname. |
| **IP address** | Sets the IP address |
| **packetlen** | (Optional) Set the length of the packet. |

This command has no default settings.

Command mode

This example shows how to trace a route to a network device named aragon:

root@localhost.cisco.com# traceroute -I -n -v -f first\_ttl -p 5 -w 10 aragon 123.34.54.12

root@localhost.cisco.com#

# traceroute6

To trace the route to a IPv6 network device, use the traceroute6 command. This command was introduced in NAM 6.0(1).

traceroute [ n | v] [-m max\_ttl] [-p port] [-s src\_addr] [-w waittime] destination host name | IPv6 address

|  |  |
| --- | --- |
| **-n** | (Optional) Prints hop addresses numerically. |
| **-v** | (Optional) Sets the output to verbose. |
| **-m max\_ttl** | (Optional) Sets the maximum time-to-live (max number of hops) used. |
| **-p port** | (Optional) Sets the base UDP port number used in probes. |
| **-s src\_addr** | (Optional) Forces the source address to be an address other than the IP address of the interface the packet is sent on. |
| **-w waittime** | (Optional) Sets the time (in seconds) to wait for a response to a probe. |

This command has no default settings.

Command mode

This example shows how to trace a route to a network device named aragon:

# trap-dest

To enter the trap destination subcommand mode and create or edit trap destinations on the NAM, use the trap-dest command. To remove a trap destination entry, use the no form of this command.

trap-dest

no trap-dest [control-index]

|  |  |
| --- | --- |
| control-index | (Optional) Specifies the collection control index. Range is from 1 to 65535.  |

This command has no default settings.

Command mode

When you enter the trap destination subcommand mode, the following commands are available:

* **address**—Sets the trap destination IP address.
* **cancel**—Discards changes and exits from the subcommand mode; see the **autocreate-data-source** section.
* community community\_string—Sets the community string.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **index** index—(Optional) Sets the trap index. Range is from 1 to 65535. Default is random.
* **owner** string—(Optional) Specifies the collection owner. Default is monitor. This option is removed in NAM 6.0(1).
* The collections that are configured in the CLI will not be visible in the GUI. For collections that use a GUI screen, you can make them visible in the GUI by using the owner string “LocalMgr.”
* **port**—(Optional) Sets the UDP port. Default is 162.

This example shows how to configure traps on the NAM:

root@hostname.cisco.com# trap-dest

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@hostname.cisco.com(sub-trap-dest)# ?

? - display help

address - set IP address (\*)

cancel - discard changes and exit from subcommand mode

community - set community string (\*)

exit - exit from subcommand mode

help - display help

index - set trap index

owner - set owner string (Removed in NAM 6.0(1))

port - set UDP port

(\*) - denotes a mandatory field for this configuration.

root@hostname.cisco.com(sub-trap-dest)# address 10.0.0.1

root@hostname.cisco.com(sub-trap-dest)# community public

root@hostname.cisco.com(sub-trap-dest)# exit

Trap created successfully.

root@hostname.cisco.com# show trap-dest

Trap index:48981

Community: public

Address: 10.0.0.1

UDP port: 162 (00a2)

Owner: monitor (Removed in NAM 6.0(1))

root@hostname.cisco.com#

**application**

**audit-trail enable**

**show trap-dest**

# upgrade

To download and install a new maintenance/application image on the NAM, use the upgrade command.

upgrade ftp://user:passwd@host/full-path/filename reformat

|  |  |
| --- | --- |
| ftp://user:passwd@host/full-path/filename*reformat* | Path to the location of the upgrade maintenance image.(Optional) Reformat the existing installation. All configuration and data will be lost. This command is the same as option 2 (-install) in the helper utility.  |

This command has no default settings.

Command mode

This example shows how to download and install a new maintenance image:

Root@localhost# upgrade ftp://alamo:nam@milton/dir65/disk/dir65/upgrade\_now

Root@localhost#

**show patches**

**show version**

# waas export server-filter-list

To export WAAS server filter list to a remote host, use the waas export server-filter-list command.

waas export server-filter-list ftp://<username:<password>@<host>/<path>

|  |  |
| --- | --- |
| ftp://<username:<password>@<host>/<path> | Specifies the remote location reachable by ftp.  |

This command has no default settings.

Command mode

The following example shows how to export the waas server filter list to a remote host:

root@nam.cisco.com# waas export server-filter-list ftp://joe@company.com//waas/configs

root@nam.cisco.com#

# waas import server-filter-list

To import the WAAS server filter list from a remote host, use the waas import server-filter-list command.

waas import server-filter-list ftp://<username:<password>@<host>/<path>/<file>

|  |  |
| --- | --- |
| ftp://<username:<password>@<host>/<path> | Specifies the remote location reachable by ftp.  |

This command has no default settings.

Command mode

The following example shows how to import the waas server filter list from a remote host:

root@nam.cisco.com#
waas import server-filter-list ftp://joe@company.com//waas/config/svrlist

root@nam.cisco.com#

# waas server filter

To add a WAAS server filter, use the waas import server-filter command. To remove a server filter, use the no form of this command

waas server filter <ip-address>

no waas server filter <ip-address>

|  |  |
| --- | --- |
| ip-address | Specifies IPV4 of the WAAS server |

This command has no default settings.

Command mode

The following example shows how to add a WAAS server filter and how to remove a WAAS server filter:

root@nam.cisco.com# waas server filter 10.0.0.2

Successfully added server filter.

root@nam.cisco.com# no waas server filter 10.0.0.2

root@nam.cisco.com#

# web-publication

To enable and set up a list of hosts that can view the NAM GUI monitoring displays without logging into the NAM, use the web-publication command. To remove web publishing from your configuration, use the no form of this command.

web-publication username

no web-publication

|  |  |
| --- | --- |
| username | Sets the username. |

This command has no default settings.

Command mode

When you enter the web user subcommand mode, the following commands are available:

* **?** or **help**—Displays help; see the **help** command.
* **cancel**—Discards changes and exits from the subcommand mode.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **alarm** enable | disable—(Optional) Enables or disables web publishing of alarm displays.
* **allow-hosts** WORD—Sets the hosts which are allowed to view web published monitoring displays.
* **code** WORD—Sets the code which allows hosts to view web published monitoring displays.
* **report** enable | disable—(Optional) Enables or disables web publishing report displays.
* **rmon** enable | disable—(Optional) Enables or disables web publishing RMON monitoring displays.
* **voice** enable | disable—(Optional) Enables or disables web publishing voice monitoring displays.

This example shows how to configure a host to receive web published reports from the NAM:

root@hostname.cisco.com# web-publication

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@hostname.cisco.com(sub-web-publication)# ?

root@hostname.cisco.com#

**show web-publication**

# web-user

To enter the web user configuration subcommand mode, and then configure local web users on the NAM, use the web-user command. To remove a web user from your configuration, use the no form of this command.

web-user

no web-user username

|  |  |
| --- | --- |
| username | Sets the username. |

This command has no default settings.

Command mode

When you enter the web user subcommand mode, the following commands are available:

* **account-mgmt** enable | disable—(Optional) Enables or disables the account management privilege.
* **alarm-config** enable | disable—(Optional) Enables or disables the alarm configuration privilege.
* **cancel**—Discards changes and exits from the subcommand mode.
* **capture** enable | disable—(Optional) Enables or disables the packet capture and decode privilege.
* **collection-config** enable | disable—(Optional) Enables or disables the collection configuration privilege.
* **exit**—Saves changes and exits from the subcommand mode; see the **exit** command.
* **system-config** enable | disable—(Optional) Enables or disables the system configuration privilege.
* **user-name** username—Sets the username.

This example shows how to configure a NAM web user:

root@hostname.cisco.com# web-user

Entering into subcommand mode for this command.

Type 'exit' to come out of this mode.

Type 'cancel' to discard changes and to come out of this mode.

root@hostname.cisco.com(sub-web-user)# ?

? - display help

account-mgmt - enable/disable account management privilege

alarm-config - enable/disable alarm configuration privilege

cancel - discard changes and exit from subcommand mode

capture - enable/disable packet capture/decode privilege

collection-config - enable/disable collection configuration privilege

exit - exit from subcommand mode

help - display help

system-config - enable/disable system configuration privilege

user-name - set username (\*)

(\*) - denotes a mandatory field for this configuration.

root@hostname.cisco.com(sub-web-user)# user-name foo

root@hostname.cisco.com(sub-web-user)# account-mgmt enable

root@hostname.cisco.com(sub-web-user)# exit

No password specified.

Do you want specify password now (y/n) [n] y

Enter password:

Confirm password:

User 'foo' created successfully.

root@hostname.cisco.com# show web-users foo

User name: foo

Account management:Enabled

System config: Disabled

Capture: Disabled

Alarm config: Disabled

Collection config: Disabled

Collection view: Enabled

root@hostname.cisco.com#

**show web-user**

# Appendix ANAM Maintenance Partition CLI\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table A-1 lists the Network Analysis Module maintenance partition commands.

|  |
| --- |
| * NAM Maintenance Image CLI
 |
| Command | Usage |
| ip address address mask | Sets the NAM IP address. |
| ip broadcast broadcast-address | Sets the NAM broadcast address. |
| ip gateway gateway-address | Sets the NAM gateway address. |
| ip nameserver DNS-server-address1 [DNS-server-address2 [DNS-server-address3]] | Sets up to three DNS server addresses. |
| ip host host-name | Sets the NAM device hostname. |
| ip domain domain | Sets the NAM device domain. |
| show ip | Shows the NAM IP parameters. |
| show images | Shows images located on the NAM application partition. |
| show version | Shows the NAM system parameters. |
| show log upgrade | Shows the upgrade log file. |
| passwd | Sets the password for the current user. |
| upgrade ftp-url [--install] | Upgrades the NAM application image. |
| ping address | Sends echo messages. |
| clear ip | Removes the NAM network configuration. |
| clear log upgrade | Clears the log file for the upgrade operation. |
| logout | Exits the current session. |
| exit | Exits the current session. |
| passwd-guest | Sets the password for the guest account. |
| enable-guest | Enables the guest account. |
| disable-guest | Disables the guest account. |
| reset | Reboots the NAM (available in guest account only). |
| upgrade-bios | Installs a new BIOS image (available in guest account only). |

# Appendix BAcronyms\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table B-1 defines the acronyms used in this publication.

|  |
| --- |
| * List of Acronyms
 |
| Acronym | Expansion |
| ARP | Address Resolution Protocol |
| ART | Application Response Time |
| CDB | circular data base, proprietary NAM database |
| CIR | committed information rate |
| CLI | command-line interface |
| DIFFSERV | differentiated services |
| DNS | Domain Name System |
| DSCP | differentiated services code point |
| DSMON | Differentiated Services Monitoring |
| FTP | File Transfer Protocol |
| GUI | Graphical User Interface |
| HTTP | HyperText Transfer Protocol |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| ISO | International Organization of Standardization |
| LAN | local area network |
| LUN | Logical unit number. A LUN results from mapping a SCSI logical unit number, port ID, and LDEV ID to a RAID group.  |
| MAC | Media Access Control |
| MD5 | message digest 5 |
| MFD | multicast fast drop |
| MGCP | Media Gateway Control Protocol |
| MIB | Management Information Base |
| MII | media-independent interface |
| MPLS | Multiprotocol Label Switching |
| MTU | maximum transmission unit |
| NAM | Network Analysis Module |
| NDE | NetFlow Data Export |
| NetBIOS | Network Basic Input/Output System |
| NTP | Network Time Protocol |
| PC | Personal Computer (formerly PCMCIA) |
| PHY | physical sublayer |
| PTP | Precision Time Protocol (1588) |
| QoS | quality of service |
| RCP | Remote Copy Protocol |
| RMON | remote network monitor |
| RPC | remote procedure call |
| RSPAN | remote SPAN |
| SCP | Switch-Module Configuration Protocol |
| SCCP | Skinny Client Control Protocol |
| SM-SRE | Service Module-Services Ready Engine  |
| SNMP | Simple Network Management Protocol |
| SPAN | Switched Port Analyzer |
| SRE | Services Ready Engine |
| SSL | Secure Sockets Layer |
| SVC | switched virtual circuit |
| TACACS+ | Terminal Access Controller Access Control System Plus |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TFTP | Trivial File Transfer Protocol |
| TOS | type of service |
| TTL | Time To Live |
| UDP | User Datagram Protocol |
| UTC | Coordinated Universal Time |
| VACL | VLAN access control list |
| VLAN | virtual LAN |
| VPN | virtual private network |
| VTP | VLAN Trunking Protocol |
| WAAS | Wide Area Application Services |
| WAN | Wide Area Network |