Cisco Prime Network Analysis Module
Command Reference Guide

Versions 5.1(2), 5.1(3), 6.0(1) and 6.0(2)
December 2013

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 HEREBY 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. 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

1: Command Line Interface  
12

2: NAM CLI Commands: application - device waas  
16

  - application  
  18
  - application group  
  19
  - audit-trail enable  
  21
  - autocreate-data-source  
  22
  - cdp enable  
  23
  - cdp hold-time  
  24
  - cdp interval  
  25
  - classification-mode default  
  26
  - classification-mode deep-inspect  
  27
  - clear access log  
  28
  - clear captured-data-files  
  29
  - clear monitoring-data  
  30
  - clear system-alerts  
  31
  - clear system-passwords  
  32
  - clock set  
  33
  - config clear  
  34
  - config network  
  36
  - config upload  
  38
  - coredump  
  40
  - data-source erspan  
  41
  - data-source netflow  
  42
  - data-source pa  
  43
  - data-source waas  
  44
  - debug log disable  
  46
  - debug log enable  
  47
  - debug log level  
  48
  - debug log metric-engine  
  50
debug log reset
device erspan
device netflow
device waas

3: NAM CLI Commands:  email – logout
email
entity alias
entity assetid
exit
exsession
ftp
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
### 4: NAM CLI Commands: metric export host - show certificate request

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric export host</td>
<td>91</td>
</tr>
<tr>
<td>metric export non-waas traffic</td>
<td>92</td>
</tr>
<tr>
<td>monitor data-aggr-intv</td>
<td>93</td>
</tr>
<tr>
<td>monitor nbar</td>
<td>95</td>
</tr>
<tr>
<td>monitor protocol encapsulation</td>
<td>96</td>
</tr>
<tr>
<td>monitor rtp-stream enable</td>
<td>97</td>
</tr>
<tr>
<td>monitor rtp-stream filter</td>
<td>98</td>
</tr>
<tr>
<td>monitor rtp-stream threshold</td>
<td>99</td>
</tr>
<tr>
<td>monitor urlcollection</td>
<td>101</td>
</tr>
<tr>
<td>monitor urlfilter</td>
<td>103</td>
</tr>
<tr>
<td>mtrace-clear, mtrace-show, mtrace-start, mtrace-stop, mtrace-upload</td>
<td>105</td>
</tr>
<tr>
<td>netflow input port</td>
<td>106</td>
</tr>
<tr>
<td>nslookup</td>
<td>107</td>
</tr>
<tr>
<td>password</td>
<td>108</td>
</tr>
<tr>
<td>password strong-policy</td>
<td>109</td>
</tr>
<tr>
<td>patch</td>
<td>110</td>
</tr>
<tr>
<td>pid-sn</td>
<td>111</td>
</tr>
<tr>
<td>ping</td>
<td>112</td>
</tr>
<tr>
<td>ping6</td>
<td>113</td>
</tr>
<tr>
<td>preferences</td>
<td>115</td>
</tr>
<tr>
<td>protocol esp-null-heuristic</td>
<td>117</td>
</tr>
<tr>
<td>reboot</td>
<td>118</td>
</tr>
<tr>
<td>reboot -helper</td>
<td>119</td>
</tr>
<tr>
<td>reboot -golden</td>
<td>120</td>
</tr>
<tr>
<td>remote-storage</td>
<td>121</td>
</tr>
<tr>
<td>remote-storage fcoe</td>
<td>122</td>
</tr>
<tr>
<td>remote-storage iscsi</td>
<td>124</td>
</tr>
<tr>
<td>remote-storage sas</td>
<td>126</td>
</tr>
<tr>
<td>remove corefiles</td>
<td>128</td>
</tr>
<tr>
<td>rise-nam enable / disable</td>
<td>129</td>
</tr>
<tr>
<td>rmwebusers</td>
<td>130</td>
</tr>
<tr>
<td>secure-clear all</td>
<td>131</td>
</tr>
</tbody>
</table>
show access-log
show application app-id
show application eng-id
show application group
show audit-trail
show autocreate-data-source
show cdb
show cdp settings
show certificate
show certificate-request

5: NAM CLI Commands: show clock details - show monitor urlfilter
show classification-settings
show clock details
show configuration
show corefiles
show counters
show cpu
show data-source
show date
show debug log-levels
show debug messages
show debug metric-engine
show debug online-diag-stats
show debug rise-messages
show decode-log
show device
show email
show entity
show ftp
show hosts
show interface management-port
show internal resources monitoring
show inventory
show ip

show license

show local-storage all

show local-storage physical

show local-storage progress

show local-storage virtual

show log config

show log patch

show log report

show log upgrade

show memory

show metric export

show monitor protocol encapsulation

show monitor protocol all

show monitor rtp-stream

show monitor rtp-stream filter

show monitor urlcollection

show monitor urlfilter

6: NAM CLI Commands: show password strong-policy - web user

show password strong-policy

show patches

show pkt-drop counters

show preferences

show protocol-feature

show remote-storage

show rxcounters

show snmp

show syslog-settings

show system-alerts

show tech-support

show time

show time ptp

show trap-dest
show top-memory-users
show version
show waas data-source
show waas device
show waas server filter
show web-publication
show web-user
shutdown
snmp
syslog
syslog remote-server
terminal
time
traceroute
traceroute6
trap-dest
upgrade
waas export server-filter-list
waas import server-filter-list
waas server filter
web-publication
web-user

Appendix A
  NAM Maintenance Partition CLI
  243

Appendix B
  Acronyms
  245
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:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>1: Command Line Interface</td>
<td>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.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>2: NAM CLI Commands: application - device waas</td>
<td>Lists CLI commands alphabetically and provides detailed information about the commands.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>3: NAM CLI Commands: email – logout</td>
<td>Lists CLI commands alphabetically and provides detailed information about the commands.</td>
</tr>
</tbody>
</table>
### Chapter 4

**NAM CLI Commands**: metric export host - show certificate request

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 A**

NAM Maintenance Partition CLI

Lists the NAM maintenance partition commands.

### Appendix B

**Appendix B**

Acronyms

Defines the acronyms used in this guide.

---

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><em>italic</em> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><code>screen</code> font</td>
</tr>
</tbody>
</table>
Information you enter | **boldface screen font**
---|---
Variables you enter | *italic screen font*
Menu items and button names | **boldface font**

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

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

**Warning** 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:


### Obtaining Documentation and Submitting a Service Request

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


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)

**Note** 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:

**Step 1** Log into the console using the Telnet connection or the console port connection.

**Step 2** 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:**
```
n7k7-mod9.cisco.com login:
    n7k7-mod9.cisco.com login:
    Step 3 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
    Step 4 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#
```
Changing the Default Password

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

**Step 1** 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.

**Step 2** Enter the new password as follows:

```
Changing password for user root
New UNIX password:
```

**Step 3** Enter the new password again as follows:

```
Retype new UNIX password:
pwd: 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:
pwd: 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:

```
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)#
```

**Note**  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) and 6.0(2) 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 – logout
- 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 added in NAM 6.0(1).
Classification-mode default

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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 is added in NAM 6.0(1).

**Classification-mode deep-inspect**

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to use deep packet inspection:

```
rroot@nam.localdomain# classification-mode deep-inspect
```

This operation 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
```

Defaults
This command has no default settings.

Command Modes
Command mode

Usage Guidelines
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 a protocol and one port or port range. Repeat `match` command if there is more than one protocol or ports need to be include in this user defined protocol.
- **name string**—Sets the application name. This is a mandatory field.

Examples
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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>group-name</th>
<th>Application group name.</th>
</tr>
</thead>
</table>

### Syntax Description

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.
Examples

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
Successfully 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#
```

Related Commands

```
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
```

**Defaults**

Audit trail of the CLI and GUI accesses is enabled.

**Command Modes**

Command mode

**Examples**

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

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

**Related Commands**

`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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

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

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

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

**Examples**
This example shows how to enable CDP:

```
root@localhost.cisco.com# cdp enable
root@localhost.cisco.com#
```

**Related Commands**
- `classification-mode default`

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

```
Classification-mode default
```

**Syntax Description**
This command has no arguments or keywords.
**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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 is added in NAM 6.0(1).

**Classification-mode deep-inspect**

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to use deep packet inspection:

```
root@nam.localdomain# classification-mode deep-inspect
This operation 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
```

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>Specifies the CDP hold time. Range is from 10 to 255 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

180 seconds.

**Command Modes**

Command mode

**Examples**

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

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

**Related Commands**

Error! Reference source not found.
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
```

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

**Syntax Description**

```
time
```

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

**Defaults**

60 seconds

**Command Modes**

Command mode

**Examples**

This example shows how to set the CDP messages interval:

```
root@localhost.cisco.com# cdp interval 200
root@localhost.cisco.com#
```

**Related Commands**

Error! Reference source not found.
classification-mode default
To use default NAM packet classification, use the classification-mode default command. This command is added in NAM 6.0(1).

Classification-mode default

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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 is added in NAM 6.0(1).

Classification-mode deep-inspect

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to use deep packet inspection:

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

This operation 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
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to clear the access log:

```
root@localhost# clear access-log
```

**Related Commands**
secure-clear all
To clean all users data before shipping, use the secure-clear all command. This is added in NAM 6.0(1).

```
Secure-clear all
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode
Examples
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

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to delete all captured files:

root@localhost# clear captured-data-files
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
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to clear the system alerts:

    root@localhost# clear system-alerts

Related Commands
show system-alerts
clear system-passwords

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

    clear system-passwords

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to clear the system passwords:

    root@localhost# clear system-passwords
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>
```

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

**Syntax Description**

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

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

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]`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>(Optional) Resets all NAM configurations to factory default including the NAM IP parameters configuration. The NAM reboots automatically for the changes to take effect.</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>(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.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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.

```plaintext
config network url [config_filename]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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.

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

```
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 #
Related Commands

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

```
config upload url [config_filename]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>url</code></td>
<td>Specifies the location of the configuration or license file to upload;</td>
</tr>
<tr>
<td></td>
<td><code>ftp://&lt;username&gt;@&lt;host&gt;/&lt;path&gt;</code></td>
</tr>
<tr>
<td><code>config_filename</code></td>
<td>Specifies the filename for the configuration file.</td>
</tr>
</tbody>
</table>

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
If `config_filename` is not specified when this command is issued, NAM will assign a default config file name.

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

```
root@NAM# config upload ftp://kluu@namlab-pcl.cisco.com example.config
Building configuration, please wait... Done.

Uploading the configuration to 'example.config'
on 'ftp://kluu@namlab-pcl.cisco.com', This may take few minutes ...

Password:

Successfully uploaded the NAM configuration.
root@NAM#
```
Related Commands

config network
**coredump**

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

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

**Syntax Description**

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

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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.

```plaintext
data-source erspan
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
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

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

```plaintext
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

Defaults
This command has no default settings.

Command Modes
Command mode

Usage Guidelines
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

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

```
rroot@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.
```

```
rroot@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

Defaults

This command has no default settings.

Command Modes

Command mode

Usage Guidelines

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

Examples

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.

```plaintext
data-source waas
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
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.

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

```plaintext
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 subcommand 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.

```
depbug log disable
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default behavior or settings.

**Command Modes**

Command mode

**Examples**

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

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default behavior or settings.

**Command Modes**
Command mode

**Examples**
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>
```

**Syntax Description**

```
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—Critical
1—Error
2—Warning
3—Notice
4—Info
5—Debug
6—Debug2
7—Debug3
```

**Defaults**

This command has no default behavior or settings.

**Command Modes**

Command mode
Examples
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.

```
default log metric-engine
```

Syntax Description
This command has no arguments or keywords.

Defaults
No default behavior or values.

Command Modes
Command mode

Examples
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

No default behavior or values.

**Command Modes**

Command mode

**Examples**

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
```

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

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
  - device IP address (*)
  - discard changes and exit from subcommand mode
  - create device and exit from sub-command mode
  - display help
  - 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
```

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

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
ext – 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

Defaults
This command has no default settings.

Command Modes
Command mode

Usage Guidelines
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.

Examples
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 – logout

This chapter provides information about the following commands:

- email
- entity alias
- entity assetid
- 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.

```plaintext
email

no email server

no email alarm
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

**Note**

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.
- `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`.

**Examples**

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.

Related Commands
show debug metric-engine
**entity alias**

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

```
entity alias string
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>String</code></td>
<td>Specifies the entity string used to configure the entPHysicalAlias.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.

**Examples**

This example shows how to log out of the NAM:

```
root@localhost# entity alias 123456
```

**Related Commands**

`show entity`
**entity assetid**

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

```
entity assetid string
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>String</strong></td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.

**Examples**

This example shows how to log out of the NAM:

```
root@localhost# entity assetid 1234566
```

**Related Commands**

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

```
exit
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

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

**Examples**
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables outside logins.</td>
</tr>
<tr>
<td>off</td>
<td>Disables outside logins.</td>
</tr>
<tr>
<td>ssh</td>
<td>(Optional) Sets the outside logins to SSH.</td>
</tr>
</tbody>
</table>

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
A strong crypto patch is required if you use the `ssh` option.

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

```
root@localhost# exsession on
```
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.

**Examples**

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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>directory</td>
<td>FTP location at the FTP server</td>
</tr>
<tr>
<td>exit</td>
<td>exit from subcommand mode</td>
</tr>
<tr>
<td>help</td>
<td>display help</td>
</tr>
<tr>
<td>index</td>
<td>a unique integer identifying the ftp entry</td>
</tr>
<tr>
<td>password</td>
<td>password of the user at the FTP server</td>
</tr>
<tr>
<td>server</td>
<td>set FTP server</td>
</tr>
<tr>
<td>user</td>
<td>user name at the FTP server</td>
</tr>
</tbody>
</table>
help

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

help | ?

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode or subcommand mode.

Examples
This example shows how to display help:

name.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 has been added in NAM 6.0(1).

```
  ip address ip-address subnet-mask
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
</tr>
<tr>
<td><code>subnet-mask</code></td>
</tr>
</tbody>
</table>

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
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.

**Examples**
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#  

Related Commands
ip broadcast
ip domain
ip host
ip broadcast

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

`ip broadcast broadcast-address`

**Syntax Description**

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

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to set the system broadcast address:

```
root@localhost# ip broadcast 172.20.104.127
root@localhost#
```

**Related Commands**

- ip broadcast
- ip domain
- ip host
- show ip
**ip domain**
To set the system domain name, use the `ip domain` command.

```
  ip domain name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Sets the system domain name.</th>
</tr>
</thead>
</table>

### Defaults
This command has no default settings.

### Command Modes
Command mode

### Examples
This example shows how to set the IP domain name:

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

### Related Commands
- `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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-gateway</code> Sets the default gateway address.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

**Command mode**

### Examples

This example shows how to set the IP gateway address:

```
root@localhost# ip gateway 123.34.56.0
```

### Related Commands

- `ip broadcast`
- `ip domain`
- `ip host`
- `show ip`
ip host

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

   ip host name

Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Sets the IP hostname.</th>
</tr>
</thead>
</table>

Defaults

This command has no default settings.

Command Modes

Command mode

Examples

This example shows how to set the IP hostname:

root@NAM.cisco.com# ip host orion
root@orion.cisco.com#

Related Commands

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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Sets the host IP address.</td>
</tr>
<tr>
<td><code>host-name</code></td>
<td>Sets the hostname which can be a FTP URL with a filename.</td>
</tr>
<tr>
<td><code>alias1 alias2</code></td>
<td>(Optional) Sets the host alias.</td>
</tr>
<tr>
<td><code>ftp://user:passwd@host/full-path/filename</code></td>
<td>Sets the path to the host parameters file location.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Usage Guidelines

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.

### Examples

This example shows how to add a specific IP host:

```
root@localhost# ip hosts add 30.50.68.10 orion
```

### Related Commands

- **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

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>Sets the host IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax Description</td>
<td>ftp://user:passwd@host/full-path/filename</td>
<td>Sets the path to the host parameters file location.</td>
</tr>
</tbody>
</table>

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to delete a specific IP host:

    root@localhost# ip hosts delete 30.50.68.10 orion

Related Commands
ip hosts add
ip http port

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

`ip http port 1-65535`

**Syntax Description**

<table>
<thead>
<tr>
<th>Port</th>
<th>Application</th>
<th>Port</th>
<th>Application</th>
<th>Port</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tcpmux</td>
<td>43</td>
<td>nicname</td>
<td>117</td>
<td>uucp-path</td>
</tr>
<tr>
<td>7</td>
<td>echo</td>
<td>53</td>
<td>domain</td>
<td>119</td>
<td>NNTP</td>
</tr>
<tr>
<td>9</td>
<td>discard</td>
<td>77</td>
<td>priv-rjs</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>11</td>
<td>systat</td>
<td>79</td>
<td>finger</td>
<td>135</td>
<td>loc-srv /</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>epmap</td>
</tr>
<tr>
<td>13</td>
<td>daytime</td>
<td>87</td>
<td>ttylink</td>
<td>139</td>
<td>netbios</td>
</tr>
<tr>
<td>15</td>
<td>netstat</td>
<td>95</td>
<td>supdup</td>
<td>143</td>
<td>IMAP2</td>
</tr>
<tr>
<td>17</td>
<td>qotd</td>
<td>101</td>
<td>hostriame</td>
<td>179</td>
<td>LDAP</td>
</tr>
<tr>
<td>19</td>
<td>chargen</td>
<td>102</td>
<td>iso-tsap</td>
<td>389</td>
<td>LDAP</td>
</tr>
<tr>
<td>20</td>
<td>ftp data</td>
<td>103</td>
<td>gppitnp</td>
<td>465</td>
<td>SMTP+SSL</td>
</tr>
<tr>
<td>21</td>
<td>ftp control</td>
<td>104</td>
<td>acr-nema</td>
<td>512</td>
<td>print / exec</td>
</tr>
<tr>
<td>22</td>
<td>ssh</td>
<td>109</td>
<td>POP2</td>
<td>513</td>
<td>login</td>
</tr>
<tr>
<td>23</td>
<td>telnet</td>
<td>110</td>
<td>POP3</td>
<td>514</td>
<td>shell</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>531</td>
<td>chat</td>
</tr>
<tr>
<td>532</td>
<td>netnews</td>
</tr>
<tr>
<td>540</td>
<td>uucp</td>
</tr>
<tr>
<td>556</td>
<td>remotefs</td>
</tr>
<tr>
<td>563</td>
<td>NNTP+SSL</td>
</tr>
<tr>
<td>587</td>
<td>submission</td>
</tr>
<tr>
<td>601</td>
<td>syslog</td>
</tr>
<tr>
<td>636</td>
<td>LDAP+SSL</td>
</tr>
<tr>
<td>993</td>
<td>IMAP+SSL</td>
</tr>
<tr>
<td>995</td>
<td>POP3+SSL</td>
</tr>
<tr>
<td>404</td>
<td>lockd</td>
</tr>
<tr>
<td>600</td>
<td>X11</td>
</tr>
</tbody>
</table>
### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

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

```
root@localhost# ip http port 233
```

### Related Commands

- `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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate-request</td>
</tr>
<tr>
<td>- Generates a certificate request.</td>
</tr>
<tr>
<td>self-signed-certificate</td>
</tr>
<tr>
<td>- Generates a self-signed certificate.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to set up a secure server:

```
root@localhost# ip http secure generate certificate-request
```

**Related Commands**

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

    ip http secure install certificate

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

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

    root@localhost# ip http secure install certificate

Related Commands
`ip`
**ip http secure port**

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

```
ip http secure port port
```

**Syntax Description**

Not all ports are available to be assigned. Most browsers block ports that are used for other applications. Commonly-Blocked Ports on page 78 lists the commonly blocked ports.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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

```
root@localhost# ip http secure port 30
```

**Related Commands**

`ip`
ip http secure server

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>server enable</th>
<th>disable</th>
<th>Enables or disables the HTTP server.</th>
</tr>
</thead>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

A strong crypto patch is required before applying this command.

**Examples**

This example shows how to set up a secure server:

```
root@localhost# ip http secure server enable
```

**Related Commands**

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

```
ip http server {enable | disable}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the HTTP server.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the HTTP server.</td>
</tr>
</tbody>
</table>

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to enable a HTTP server:

```
root@localhost# ip http server enable
```

**Related Commands**

- 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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the TACACS+ server.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the TACACS+ server.</td>
</tr>
<tr>
<td>primary-srv</td>
<td>Specifies the primary TACACS+ server.</td>
</tr>
<tr>
<td>backup-srv</td>
<td>(Optional) Specifies the backup TACACS+ server.</td>
</tr>
<tr>
<td>en-secret-key</td>
<td>(Optional) Argument name to enable the secret key.</td>
</tr>
<tr>
<td>encrypted-secret-key</td>
<td>(Optional) Argument value.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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="
```

**Examples**

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#

**Related Commands**

*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
```

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

### Syntax Description

| **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. |

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
This command is supported only on the NME-NAM.

**Examples**

```
root@localhost# ip interface external
```

**Related Commands**

- **ip**
- **show ip**
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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-addr</code></td>
<td>Sets the name server address.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables the name server entries.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

This example shows how to set a system name server:
```
root@localhost# ip nameserver 171.69.2.133
```

### Related Commands

`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

Syntax Description

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

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Command mode

Usage Guidelines

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

Examples

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
```

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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` is added in NAM 6.0(1).

```
no managed-device address
managed-device address <ip-address>
```

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

**Syntax Description**

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

**Defaults**

No default behavior or values.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

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 manage-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 is added in NAM 6.0(1).

```plaintext
No managed-device community

**managed-device community** <rw-community>
```

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

**Syntax Description**

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

**Defaults**

None.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

The following example sets the managed-device community:

```plaintext
root@nam.cisco.com# managed-device community
root@nam.cisco.com# managed-device community
root@nam.localdomain# no managed-device community
Managed Device Community string removed if any!
root@nam.localdomain#
```
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 is added in NAM 6.0(1).

Default data-aggr-intv

This command has no default settings.

Command Modes
Command mode

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

- ?—Displays help. (Added 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. (added 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).

**Examples**

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**
- **pid-sn**
- **ping**
- **preferences**
- **protocol esp-null-heuristic**
• reboot
• reboot -helper
• reboot -golden
• remote-storage
• remote-storage fcoe
• remote-storage iscsi
• remote-storage sas
• rmwebusers
• show access-log
• show application app-id
• show application eng-id
• show application group
• show audit-trail
• show autocreate-data-source
• show cdb
• show cdp settings
• show certificate
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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
</tr>
<tr>
<td><strong>port</strong></td>
</tr>
</tbody>
</table>

### Defaults

The default port is 9995.

### Command Modes

Command mode

### Usage Guidelines

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

### Examples

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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Export is disabled.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

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 is added in NAM 6.0(1).

```
Monitor data-aggr-intv
```

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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

- `?`—Displays help. (Added 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. (added 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-rsp-time [min]`—Specify short term interval for application response time (min).
- `short-term-traffic [min]`—Specify short term interval for traffic/media (min).

**Examples**

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.

```
monitor nbar
no monitor nbar
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no defaults.

**Command Modes**
Command mode

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

**Examples**
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Related Commands**

- `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
```

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Related Commands**

`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`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>source-address</code></td>
<td>Specifies the source address of the RTP stream being filtered.</td>
</tr>
<tr>
<td><code>source-mask</code></td>
<td>Specifies the subnet mask of the source address of the RTP stream being filtered.</td>
</tr>
<tr>
<td><code>dest-address</code></td>
<td>Specifies the destination address of the RTP stream being filtered.</td>
</tr>
<tr>
<td><code>dest-mask</code></td>
<td>Specifies the subnet mask of the RTP stream being filtered.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Related Commands**

- `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>
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Word</strong></td>
</tr>
<tr>
<td>actual-pkt-loss</td>
</tr>
<tr>
<td>adjusted-pkt-loss</td>
</tr>
<tr>
<td>jitter</td>
</tr>
<tr>
<td>mos</td>
</tr>
<tr>
<td>soc</td>
</tr>
<tr>
<td>ssc</td>
</tr>
</tbody>
</table>

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
This command is supported on all NAM platforms.
Examples
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
```

Syntax Description
This command has no keywords or arguments.

Defaults
This command has no default settings.

Command Modes
Command mode

Usage Guidelines
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.

**Examples**

This example shows how to configure URL collection:

```bash
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)#
```

**Related Commands**

*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
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>control-index</code></th>
<th>Specifies the collection control index. Range is from 1 to 65535.</th>
</tr>
</thead>
</table>

**Syntax Description**

**Defaults**
The control index is random.

**Command Modes**
Command mode

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

- `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.

### Examples
This example shows how to configure URL filters:

```bash
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
Successfully created urlfilter entry.
```

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

```bash
root@nam# no monitor urlfilter 2
Successfully delete urlfilter entry.
```

### Related Commands
- `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

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

Defaults
These commands have no default settings.

Command Modes
Command mode

Examples
**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]
```

**Note**
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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port</code></td>
<td>Specifies the input UDP port number, valid values 1 - 65535.</td>
</tr>
</tbody>
</table>

**Defaults**
The default port is 3000.

**Command Modes**
Command mode

**Examples**
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]

### Syntax Description

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

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

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

**Syntax Description**

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

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
There are only two valid users, root and guest.

**Examples**
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
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
There are only two valid users, root and guest.

**Examples**
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 \texttt{patch} command.

\texttt{patch \textit{ftp://user:passwd@host/full-path/filename}}

\begin{tabular}{|p{15cm}|}
\hline
\textbf{Syntax Description} \\
\hline
\textit{ftp://user:passwd@host/full-path/file name} \hspace{1cm} Sets the path to download the patch. \\
\hline
\end{tabular}

\textbf{Defaults} \\
This command has no default settings.

\textbf{Command Modes} \\
Command mode

\textbf{Examples} \\
This example shows how to download and install a patch:

\begin{verbatim}
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#
\end{verbatim}

\textbf{Related Commands} \\
\texttt{show patches} \\
\texttt{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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIDnnnn</strong></td>
</tr>
<tr>
<td>Specifies the Product ID of the WAE device.</td>
</tr>
<tr>
<td><strong>SNnnnn</strong></td>
</tr>
<tr>
<td>Specifies the serial number of the WAE device.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

This command is valid only on NAM Virtual Blade platforms.

**Examples**

This example shows how to enter 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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
<td>(Optional) Displays the network addresses as numbers.</td>
</tr>
<tr>
<td>-v</td>
<td>(Optional) Specifies verbose output.</td>
</tr>
<tr>
<td>-c count</td>
<td>(Optional) Stops the ping after sending the count of ECHO_REQUEST packets.</td>
</tr>
<tr>
<td>-i wait</td>
<td>(Optional) Specifies the time interval in seconds between sending each packet.</td>
</tr>
<tr>
<td>-p pattern</td>
<td>(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.</td>
</tr>
<tr>
<td>-s packetsize</td>
<td>(Optional) Sets the 8 bytes of ICMP header data.</td>
</tr>
<tr>
<td>hostname</td>
<td>Sets the hostname of the network device to ping.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specifies the IP address of the network device to ping.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

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 is added in NAM 6.0(1).


Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
<td>(Optional) Displays the network addresses as numbers.</td>
</tr>
<tr>
<td>-v</td>
<td>(Optional) Specifies verbose output.</td>
</tr>
<tr>
<td>-c count</td>
<td>(Optional) Stops the ping6 after sending the count of ECHO_REQUEST packets.</td>
</tr>
<tr>
<td>-i wait</td>
<td>(Optional) Specifies the time interval in seconds between sending each packet.</td>
</tr>
<tr>
<td>-p pattern</td>
<td>(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.</td>
</tr>
<tr>
<td>-s packetsize</td>
<td>(Optional) Sets the 8 bytes of ICMP header data.</td>
</tr>
<tr>
<td>-I interface</td>
<td>(Optional) Sets the name of the specific interface. When pinging IPv6 Link-local address this option is required.</td>
</tr>
<tr>
<td>-M hint</td>
<td>(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.</td>
</tr>
</tbody>
</table>

Defaults

This command has no default settings.

Command Modes

Command mode
Examples
This example shows how to check the connectivity of a network device with ping6:
preferences

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

preferences

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Usage Guidelines
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 | spaces-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.
- **resolve-hostname enable | disable**—(Optional) Enables or disables hostname resolution. Default is enable.
- **Audit-trail enable | disable**—Enables or disables audit trail. This is added in NAM 6.0(1).
- **Capture-format enc**—set enc as capture format. This is added in NAM 6.0(1).
- **Capture-format pcap**—set pcap as capture format. This is added in NAM 6.0(1).

### Examples

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
```

### Related Commands

- `show preferences`
**protocol esp-null-heuristic**

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

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

```
protocol esp-null-heuristic enable
```

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

```
no protocol esp-null-heuristic enable
```

**Syntax Description**
This command enables and disables heuristic parsing of ESP-NUL packets.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to reboot to helper image:

```
root@localhost# reboot -golden
Reboot the NAM? (Y/N) [N]:
root@localhost#
```
remote-storage

Related Commands
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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name for the FCoE remote storage being removed.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Usage Guidelines

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.
### Examples
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-pwn - 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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
</tr>
<tr>
<td>Specifies the name for the iSCSI remote storage being removed.</td>
</tr>
</tbody>
</table>

**Note**

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

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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 is added in NAM 6.0(1).
Examples
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-qn- 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-qn:

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

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
Type: LUN
Model: NEXSAN SATABeast2
LUN: 2
Capacity: 1.82TB
Available: 1.73TB

Active iSCSI Sessions:
root@hostname.cisco.com#

Related Commands
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>name</th>
<th>Specifies the name of the SAS remote storage being removed.</th>
</tr>
</thead>
</table>

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.

**Examples**

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 is added in NAM 6.0(1).

Remove corefiles

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to remove all existing core files:

    root@nam.localdomain# remove corefiles
    root@nam.localdomain#

Related Commands
show corefiles
rise-nam enable / disable

To enable or disable nam rise interface, use the \texttt{rise-nam enable / disable} command. This is added in NAM 6.0(2) and currently only works on NAM 2300 appliances.

\texttt{rise-nam enable | disable}

\begin{tabular}{|l|p{0.8\textwidth}|}
\hline
\textit{Syntax Description} & \\
\hline
\texttt{disable} & disable RISE for NAM appliance. \\
\texttt{enable} & enable RISE for NAM appliance. \\
\hline
\end{tabular}

\textbf{Defaults}

default is disable for 6.0(2).

\textbf{Command Modes}

Command mode

\textbf{Examples}

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

\begin{verbatim}
root@nam.localdomain# rise-nam enable
root@nam.localdomain# rise-nam disable
\end{verbatim}

\textbf{Related Commands}
rmwebusers
To remove all web users from the local web user database, use the rmwebusers command.

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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#

Related Commands
show web-user
secure-clear all

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

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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
```

**show application app-id**

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

```
show application app-id
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to display all applications:

```
root@NAM.cisco.com# show application app-id
sample-13:1 (16777217) icmp
sample-13:2 (16777218) igmp
sample-13:4 (16777220) ip
sample-13:6 (16777222) tcp
sample-13:8 (16777224) egp
```

**Related Commands**

`application`
show application eng-id

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

  show application eng-id

Defaults
This command has no default settings.

Command Modes
Command mode

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

root@NAM.cisco.com# show application eng-id 1
sample-13:1 (16777217) icmp
sample-13:2 (16777218) igmp
sample-13:4 (16777220) ip
sample-13:6 (16777222) tcp
sample-13:8 (16777224) egp

Related Commands
application
**show application group**

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

```
show application group [group-name]
```

### Syntax Description

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

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

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
   - ftsp
     16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.3.222.4.0.1.0.0
   - ftsp-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)
     16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.190.4.0.1.0.0
   - 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)
     16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.24.113.4.0.1.0.0
   - winmx(tcp)
```
16.1.0.0.1.0.0.8.0.0.0.6.0.0.26.43.4.0.1.0.0
- edonkey(udp)
16.1.0.0.1.0.0.8.0.0.0.17.0.0.18.57.4.0.1.0.0
- edonkey(tcp)
16.1.0.0.1.0.0.8.0.0.0.6.0.0.18.53.4.0.1.0.0
- hotline
16.1.0.0.1.0.0.8.0.0.0.6.0.0.21.124.4.0.1.0.0
- soulseek
16.1.0.0.1.0.0.8.0.0.0.8.186.4.0.1.0.0
- directconnect
16.1.0.0.1.0.0.8.0.0.0.1.155.4.0.1.0.0
- bittorrent
16.1.0.0.1.0.0.8.0.0.0.6.0.0.26.225.4.0.1.0.0

Application Group: Web
Number of Protocols: 2
- http
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.80.4.0.1.0.0
- https
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.1.187.4.0.1.0.0

Application Group: Database
Number of Protocols: 9
- sql*net
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.66.4.0.1.0.0
- sqlserv(udp)
  16.1.0.0.1.0.0.8.0.0.0.17.0.0.118.4.0.1.0.0
- sqlserv(tcp)
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.118.4.0.1.0.0
- ms-sql-mon(udp)
  16.1.0.0.1.0.0.8.0.0.0.17.0.0.5.154.4.0.1.0.0
- ms-sql-mon(tcp)
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.5.154.4.0.1.0.0
- ms-sql-ser(udp)
  16.1.0.0.1.0.0.8.0.0.0.17.0.0.5.153.4.0.1.0.0
- ms-sql-ser(tcp)
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.5.153.4.0.1.0.0
- oracle-server(udp)
  16.1.0.0.1.0.0.8.0.0.0.17.0.0.5.245.4.0.1.0.0
- oracle-server(tcp)
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.5.245.4.0.1.0.0

Application Group: email
Number of Protocols: 7
- smtp
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.25.4.0.1.0.0
- smtps
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.1.209.4.0.1.0.0
- pop3(udp)
  16.1.0.0.1.0.0.8.0.0.0.17.0.0.110.4.0.1.0.0
- pop3(tcp)
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.110.4.0.1.0.0
- pop3s
  16.1.0.0.1.0.0.8.0.0.0.3.227.4.0.1.0.0
- imap2
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.143.4.0.1.0.0
- imaps
  16.1.0.0.1.0.0.8.0.0.0.6.0.0.3.225.4.0.1.0.0

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

Related Commands

application
show audit-trail

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

    show audit-trail

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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#

Related Commands
audit-trail enable
**show autocreate-data-source**

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

```
show autocreate-data-source
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
ERSSPAN 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
### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Filename</code></td>
<td>Specifies the CDB filename.</td>
</tr>
<tr>
<td><code>ARTCltsvr</code></td>
<td>IAP Client-Server table</td>
</tr>
<tr>
<td><code>ARTSiteClt</code></td>
<td>IAP Site-Client table</td>
</tr>
<tr>
<td><code>ARTSiteClt_lt</code></td>
<td>IAP Site-Client Long-Term table</td>
</tr>
<tr>
<td><code>ARTSiteSvr</code></td>
<td>IAP Site-Server table</td>
</tr>
<tr>
<td><code>ARTSiteSvr_lt</code></td>
<td>IAP Site-Server Long-Term table</td>
</tr>
<tr>
<td><code>AlarmMessages</code></td>
<td>Alarm Messages table</td>
</tr>
<tr>
<td><code>CoreConv</code></td>
<td>Conversation table</td>
</tr>
<tr>
<td><code>DataSourceStats</code></td>
<td>Data Source Stats table</td>
</tr>
<tr>
<td><code>DataSourceStats_lt</code></td>
<td>Data Source Stats Long-Term table</td>
</tr>
<tr>
<td><code>Hosts</code></td>
<td>Host table</td>
</tr>
<tr>
<td><code>Hosts_lt</code></td>
<td>Host Long-Term table</td>
</tr>
<tr>
<td><code>MDIfStats</code></td>
<td>Managed Device Interface Stats table</td>
</tr>
<tr>
<td><code>MDIfStats_lt</code></td>
<td>Managed Device Interface Stats Long-Term table</td>
</tr>
<tr>
<td><code>RtpConv</code></td>
<td>RTP Stream table</td>
</tr>
<tr>
<td><code>RtpMos</code></td>
<td>RTP MOS Quality table</td>
</tr>
<tr>
<td><code>RtpMos_lt</code></td>
<td>RTP MOS Quality Long-Term table</td>
</tr>
<tr>
<td><code>SiteMatrix</code></td>
<td>Site Matrix table</td>
</tr>
<tr>
<td><code>SiteMatrix_lt</code></td>
<td>Site Matrix Long-Term table</td>
</tr>
<tr>
<td><code>SiteStats</code></td>
<td>Site Stats table</td>
</tr>
<tr>
<td><code>SiteStats_lt</code></td>
<td>Site Stats Long-Term table</td>
</tr>
<tr>
<td><code>VolPcalls</code></td>
<td>Voice Signaling Data table</td>
</tr>
<tr>
<td><code>file-list</code></td>
<td>List CDB files</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode
**Examples**

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

```
root@nam.localdomain# show cdb
<FILENAME> - File to examine (e.g. Hosts)
ARTClitSvr - 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.

```plaintext
show cdp settings
```

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

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

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

**Examples**
To display the current CDP settings:

```plaintext
root@nam# show cdp settings
CDP is disabled
   Message Interval:   60
   Message Hold Time:  180

root@nam#
```

**Related Commands**
- `autocreate-data-source`
- `cdp hold-time`
- `cdp interval`
show certificate

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

show certificate

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to display certificate information:

```
Root@localhost# show certificate
-----BEGIN CERTIFICATE-----
MIIDgzCCAuygAwIBAgIBADANBgkqhkiG9w0BAQQFADBjJjElMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMQswCQYDVQQHEwJTSjEbMBkGA1UEChMSQ2lzY28gU3lzdGVt
cywswS5JMSswKQYDVQQELEMJYRhBhIzdCA2MDAwIE5BTSBUZUENlcnRpZmlj
YXRlMRswGQYDVQQDEwJVUzELMAkGA1UEBhMCQ0Ex
-----END CERTIFICATE-----
```

**Related Commands**

show certificate-request
show certificate-request

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

```
show certificate-request
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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

```
Root@localhost# show certificate-request
```

**Related Commands**

`show certificate`
5: NAM CLI Commands:

to show

classification-settings

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 is added in NAM 6.0(1).

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

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

root@nam.localdomain# show classification-settings
Classification method: Default
root@nam.localdomain#
show clock details

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

```
show clock details
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

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

- Reports
- CLI users
- Supervisor engine community strings

Examples
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 is added in NAM 6.0(1).

```
  show corefiles
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

### Syntax Description

This command has no arguments or keywords.

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

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

```
root@nam235Cat6k.cisco.com# show counters ?
long-term             - show long-term collection counters
nde-export            - show collection counters for NDE export
short-term             - show short-term collection counters
```
**show cpu**

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

```
show cpu
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

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

    Root@localhost# show date
    Tue Apr 26 00:14:18 2011

Related Commands
show time
time
**show debug log-levels**

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

```
show debug log-levels
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default behavior or settings.

**Command Modes**

Command mode

**Examples**

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.

```plaintext
show debug messages
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default behavior or settings.

**Command Modes**

Command mode

**Examples**

The following example shows the log file contents:

```plaintext
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-engine` command.

```
show debug metric-engine
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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-stats` command.

```
show debug online-diag-stats
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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-messages` command. This command is added in NAM 6.0(1).

```
show debug rise-messages
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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 is added in 6.0(2).

```
show decode-log
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to display the packet decode log:

```
Root@localhost# show decode-log
Jan 17 23:47:51 nam-NAM[4878]: Doing Startup
Jan 17 23:47:51 nam-NAM[4878]: build_capture_file_tables: The capture filename is 'test1_1.pcap'
Jan 17 23:47:51 nam-NAM[4878]: update_table_building_status_thread started
Jan 17 23:47:51 nam-NAM[4878]: update_table_building_status_thread finished
Jan 17 23:48:01 nam-NAM[4878]: get_capture-file-info, "filename": "test1_1.pcap", "numOfPoints":200, "includeHistogram":1", 'rx 131
Jan 17 23:48:02 nam-NAM[3911]: get_packet_summary_header_info: end of file for pktnum 50053 - Success
Jan 17 23:48:02 nam-NAM[3911]: update_table_building_status_thread finished
```

This example shows how to display the packet decode log:
**show device**

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

```
show device
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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#
```

**Related Commands**
- `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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to display entity values:

```
root@localhost# show entity
Serial Number : SAD061506JU
Alias          :
Asset ID       :
```

**Related Commands**

- `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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Command mode

Examples

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 is added in NAM 6.0(1).

```
show interface management-port
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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 is added in NAM 6.0(2).

```
show internal resources monitoring
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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 : 400000 (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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

No default behavior or values.

**Command Modes**

Command mode

**Usage Guidelines**

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

**Examples**

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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Related Commands**

- `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
```

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

### Syntax Description
This command has no arguments or keywords.

### Defaults
This command has no default settings.

### Command Modes
Command mode

### Usage Guidelines
This command is valid only on the NAM Virtual Blade.

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

```
Root@localhost# show license
```

### Related Commands
- `license install`
- `config upload`
**show local-storage all**
To show all physical disks and virtual drives, use the `show local-storage all` command.

```bash
show local-storage all
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

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

```bash
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 C02
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: 9XG1021BST91000640NS C02
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
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: 9XG02TCRST91000640NS
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
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
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

Related Commands
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 physical` command.

### Syntax Description
This command has no arguments or keywords.

### Defaults
This command has no default settings.

### Command Modes
Command mode

### Examples
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: 9XG101Y45T9100064DNS
FDE Capable: Not Capable
FDE Enable: Disable
Secured: Unsecured
Locked: Unlocked
Needs ERM 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: 9XG102M35T9100064DNS
FDE Capable: Not Capable
FDE Enable: Disable
Secured: Unsecured
Locked: Unlocked
Needs ERM 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: 9XG10CNKST9100064DNS
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
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
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
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
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

Related Commands
  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**

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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(Enc1-64 Slot-0) is not in rebuild process
Device(Enc1-64 Slot-1) is not in rebuild process
Device(Enc1-64 Slot-2) is not in rebuild process
Device(Enc1-64 Slot-3) is not in rebuild process
Device(Enc1-64 Slot-4) is not in rebuild process
Device(Enc1-64 Slot-5) is not in rebuild process
Device(Enc1-64 Slot-6) is not in rebuild process
Device(Enc1-64 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
```

Related Commands
**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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Related Commands**

- 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
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

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

```
Root@localhost# show log config
```

**Related Commands**
- `config clear`
- `show log report`
- `upgrade`
show log patch
To display the patch log entries, use the show log patch command.

show log patch

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to display the maintenance image import log entries:
Root@localhost# show log patch

Related Commands
config clear
show log report
upgrade
show log report
To display the import log entries, use the show log report command.

show log report

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to display the import log entries:

Root@localhost# show log report

Related Commands
show log config
show log upgrade

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

show log upgrade

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

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

Root@localhost# show log upgrade
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 : Verifying the image...
Fri Aug 23 10:32:30 2002 : Successfully verified the 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 : Number of Sectors: 31
Fri Aug 23 10:33:18 2002 : Successfully wrote the maint image.
Fri Aug 23 10:33:18 2002 : Performing post install...

Related Commands
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

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to display the NAM memory:

    Root@localhost# show memory
    Installed:     858 MB
    Available:     240 MB
    System Usage:  617 MB

Related Commands
show cdb
show metric export

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

```
show metric export
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

No default behavior or values.

**Command Modes**

Command mode

**Examples**

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
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to display the encapsulation configurations:

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

**Related Commands**
`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

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Command mode

Usage Guidelines
This command is supported on all NAM platforms.

Examples
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to display the RTP-stream monitoring settings and alarm thresholds.

```
root@localhost# show monitor rtp-stream
root@localhost#
```

**Related Commands**

- `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

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to display the URL collection statistics:

```
root@localhost# show monitor rtp-stream filter
root@localhost#
```

**Related Commands**
monitor rtp-stream filter
**show monitor urlcollection**

To display the URL collection configuration, use the **show monitor urlcollection** command.

```
show monitor urlcollection
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to display the URL collection statistics:

```
root@localhost# show monitor urlcollection
root@localhost#
```

**Related Commands**

`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]`

**Syntax Description**

- `control-index` (Optional) Specifies the URL filter control index.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to display the URL filter configuration:

```
root@localhost# show monitor urlfilter
root@localhost#
```

**Related Commands**

`monitor urlfilter`
6: NAM CLI Commands: show password strong-policy - web user

This chapter describes the following NAM CLI commands:

- show password strong-policy
- show patches
- show pkt-drop counters
- show preferences
- show protocol-feature
- show remote-storage
- show rxcounters
- show snmp
- show syslog-settings
- show system-alerts
- show tech-support
- show time
- show time ptp
- show trap-dest
- show version
- show waas data-source
- show waas device
- show waas server filter
- show web-publication
- show web-user
- shutdown
- snmp
- syslog
- syslog remote-server
- terminal
- time
- traceroute
- trap-dest
- upgrade
- waas export server-filter-list
- waas import server-filter-list
- waas server filter
- web-publication
- web-user
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
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
There are only two valid users, root and guest.

**Examples**
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

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to display all of the installed patches:

```
Root@localhost# show patches
```

**Related Commands**
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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#

**Related Commands**
preferences
show protocol-feature

To display the parsing protocol feature, use the `show protocol-feature` command.

```
show protocol-feature
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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
```

**Syntax Description**

This command has no keywords or arguments.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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.

```bash
show snmp
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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
```

**Related Commands**

```
show snmp
```
**show syslog-settings**

To display the NAM system log settings, use the `show syslog-settings` command.

```
show syslog-settings
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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#
```

**Related Commands**

`syslog`
**show system-alerts**

To display NAM failures or problems, use the **show system-alerts** command.

```
show system-alerts
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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 15:07:33 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 received.
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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
```

**Related Commands**
- `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`

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.

**Examples**

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]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trigger-index</td>
</tr>
</tbody>
</table>

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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#

Related Commands
traceroute6
To trace the route to a IPv6 network device, use the traceroute6 command. This command is added in NAM 6.0(1).

traceroute [n | v] [-m max_ttl] [-p port] [-s src_addr] [-w waittime] destination host name | IPv6 address

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
</tr>
</tbody>
</table>
-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.

Syntax Description

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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 is added in NAM 6.0(1).

```
show top-memory-users
```

**Syntax Description**
This command has no keywords or arguments.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
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#
```

**Related Commands**
**show version**

To display the NAM version information, use the **show version** command.

```
show version
```

**Syntax Description**

This command has no keywords or arguments.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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#
```

**Related Commands**

- `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]`

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>datasrc-index</code></td>
</tr>
</tbody>
</table>

**Defaults**
The default behavior is to show all WAAS data sources unless a specific data source index is specified.

**Command Modes**
Command mode

**Usage Guidelines**
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.

**Examples**
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.

```bash
show waas device [ip-address]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the WAAS device (optional)</td>
</tr>
</tbody>
</table>

### Defaults

The default behavior is to show all WAAS devices unless IP address is specified.

### Command Modes

Command mode

### Usage Guidelines

This command is supported on all NAM platforms.

### Examples

The following example shows the system inventory information:

```bash
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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

Syntax Description
This command has no keywords or arguments.

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to display the web user information:

    Root@localhost# show web-publication
    Web publication: enabled
    Allowed hosts: enabled
    Access code:
    Alarm screens: disabled
    Report screens: enabled
    Voice screens: enabled
    RMON screens: enabled

Related Commands
web-publication
**show web-user**

To display the web user information, use the **show web-user** command.

```
show web-user [username]
```

**Syntax Description**

- **username** (Optional) Displays the specified user name information.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

**Related Commands**

- **web-user**
**shutdown**
To shut down the NAM, use the `shutdown` command.

```
shutdown
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to shut down the NAM:

```
Root@localhost# shutdown
Shut down the NAM? (y/n) [n]: n
```

**Related Commands**
`exit`
`logout`
`preferences`
To configure NAM system MIB objects, use the **snmp** command.

```
  snmp community community-string { ro | rw }
  snmp delete community community-string
  snmp contact contact-string
  snmp location location-string
  snmp name name-string
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`community community-string { ro</td>
<td>rw }`</td>
</tr>
<tr>
<td><code>delete community-string</code></td>
<td>Deletes the device community string.</td>
</tr>
<tr>
<td><code>contact contact-string</code></td>
<td>Sets the device contact string.</td>
</tr>
<tr>
<td><code>location location-string</code></td>
<td>Sets the device location.</td>
</tr>
<tr>
<td><code>name name-string</code></td>
<td>Sets the device name.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

This example shows how to configure NAM system MIB objects:

```
Root@localhost# snmp community askdfhtjlks.01
contact george location frisco, name al
```

### Related Commands

`show snmp`
syslog

To enter the system log subcommand mode, and then configure system logging for the NAM, use the **syslog** command.

```
syslog
```

**Syntax Description**
This command has no arguments or keywords.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Usage Guidelines**
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.

**Examples**
This example shows how to configure system logging for the NAM:

```
Root@localhost# syslog
root@localhost.cisco.com(sub-syslog)#
```

**Related Commands**
```
show syslog-settings
```
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]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables remote server event logging.</td>
</tr>
<tr>
<td>server1 server2 server3 server4 server5</td>
<td>(Optional) Specifies the remote server.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

- Syslog subcommand mode

### Usage Guidelines

This command is supported on all NAM platforms.

### Examples

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.
```

### Related Commands

- `audit-trail enable`
- `show syslog-settings`
- `syslog`
**terminal**

To set the number of lines on a screen for this session, use the `terminal` command.

```
terminal editor [enable | disable]
terminal length length
terminal mode { 0 | 1}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**editor [enable</td>
</tr>
<tr>
<td><strong>length length</strong></td>
</tr>
<tr>
<td>**mode { 0</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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.
```

**Related Commands**

- `config clear`
**time**

To enter the time configuration subcommand mode, and then configure NAM system time settings, use the `time` command.

```
time
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Types**

Switch command

**Command Modes**

Privileged

**Usage Guidelines**

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.

**Examples**

This example shows how to configure system time settings on the NAM to synchronize 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
```

Related Commands

```
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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[-I]</code></td>
<td>(Optional) Specifies that ICMP ECHO is used instead of UDP datagrams.</td>
</tr>
<tr>
<td><code>[-n]</code></td>
<td>(Optional) Prints hop addresses numerically.</td>
</tr>
<tr>
<td><code>[-v]</code></td>
<td>(Optional) Sets the output to verbose.</td>
</tr>
<tr>
<td><code>[-f first_ttl]</code></td>
<td>(Optional) Sets the initial time-to-live used in the first outgoing packet.</td>
</tr>
<tr>
<td><code>[-m max_ttl]</code></td>
<td>(Optional) Sets the maximum time-to-live (max number of hops) used.</td>
</tr>
<tr>
<td><code>[-p port]</code></td>
<td>(Optional) Sets the base UDP port number used in probes.</td>
</tr>
<tr>
<td><code>[-s src_addr]</code></td>
<td>(Optional) Forces the source address to be an address other than the IP address of the interface the packet is sent on.</td>
</tr>
<tr>
<td><code>[-t tos]</code></td>
<td>(Optional) Sets the type-of-service in packets to the following value.</td>
</tr>
<tr>
<td><code>[-w waittime]</code></td>
<td>(Optional) Sets the time (in seconds) to wait for a response to a probe.</td>
</tr>
<tr>
<td><code>destination</code></td>
<td>Sets the packet destination.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Sets the host.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Sets the hostname.</td>
</tr>
<tr>
<td><code>IP address</code></td>
<td>Sets the IP address</td>
</tr>
<tr>
<td><code>packetlen</code></td>
<td>(Optional) Set the length of the packet.</td>
</tr>
</tbody>
</table>
Syntax Description

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
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 is added in NAM 6.0(1).

```
traceroute [ n | v ] [-m max_ttl] [-p port] [-s src_addr] [-w waittime] destination host name | IPv6 address
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-n</code></td>
<td>(Optional) Prints hop addresses numerically.</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>(Optional) Sets the output to verbose.</td>
</tr>
<tr>
<td><code>-m max_ttl</code></td>
<td>(Optional) Sets the maximum time-to-live (max number of hops) used.</td>
</tr>
<tr>
<td><code>-p port</code></td>
<td>(Optional) Sets the base UDP port number used in probes.</td>
</tr>
<tr>
<td><code>-s src_addr</code></td>
<td>(Optional) Forces the source address to be an address other than the IP address of the interface the packet is sent on.</td>
</tr>
<tr>
<td><code>-w waittime</code></td>
<td>(Optional) Sets the time (in seconds) to wait for a response to a probe.</td>
</tr>
</tbody>
</table>

#### Defaults

This command has no default settings.

#### Command Modes

Command mode

#### Examples

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]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>control-index</th>
<th>(Optional) Specifies the collection control index. Range is from 1 to 65535.</th>
</tr>
</thead>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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).

**Note** 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.
Examples

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-dest)# ?
? - display help
address - set IP address (*)
cancel - discard changes and exit from subcommand mode
community - set community string (*)
ext - 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-dest)# address 10.0.0.1
root@hostname.cisco.com(sub-dest)# community public
root@hostname.cisco.com(sub-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: monitoring (Removed in NAM 6.0(1))
```

Related Commands

- 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
```

### Syntax Description

<table>
<thead>
<tr>
<th>ftp://user:passwd@host/full-path/filename</th>
<th>Path to the location of the upgrade maintenance image.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>reformat</code></td>
<td>(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.</td>
</tr>
</tbody>
</table>

### Defaults

This command has no default settings.

### Command Modes

Command mode

### Examples

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#
```

### Related Commands

- `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>
```

**Syntax Description**

```
ftp://<username:<password>@<host>/<path>  
```

Specifies the remote location reachable by ftp.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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>
```

Syntax Description

```
ftp://<username>:<password>@<host>/<path>
```

Specifies the remote location reachable by ftp.

Defaults

This command has no default settings.

Command Modes

Command mode

Examples

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>
```

**Syntax Description**

<table>
<thead>
<tr>
<th>ip-address</th>
<th>Specifes IPV4 of the WAAS server</th>
</tr>
</thead>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>username</strong></td>
<td>Sets the username.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Usage Guidelines**

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.
**Examples**
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#
```

**Related Commands**

* 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

Syntax Description

username

Sets the username.

 Defaults

This command has no default settings.

Command Modes

Command mode

Usage Guidelines

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.
Examples
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

Related Commands
show web-user
Appendix A
NAM Maintenance Partition CLI

Table A-1 lists the Network Analysis Module maintenance partition commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address address mask</td>
<td>Sets the NAM IP address.</td>
</tr>
<tr>
<td>ip broadcast broadcast-address</td>
<td>Sets the NAM broadcast address.</td>
</tr>
<tr>
<td>ip gateway gateway-address</td>
<td>Sets the NAM gateway address.</td>
</tr>
<tr>
<td>ip nameserver DNS-server-address1 [DNS-server-address2 [DNS-server-address3]]</td>
<td>Sets up to three DNS server addresses.</td>
</tr>
<tr>
<td>ip host host-name</td>
<td>Sets the NAM device hostname.</td>
</tr>
<tr>
<td>ip domain domain</td>
<td>Sets the NAM device domain.</td>
</tr>
<tr>
<td>show ip</td>
<td>Shows the NAM IP parameters.</td>
</tr>
<tr>
<td>show images</td>
<td>Shows images located on the NAM application partition.</td>
</tr>
<tr>
<td>show version</td>
<td>Shows the NAM system parameters.</td>
</tr>
<tr>
<td>show log upgrade</td>
<td>Shows the upgrade log file.</td>
</tr>
<tr>
<td>passwd</td>
<td>Sets the password for the current user.</td>
</tr>
<tr>
<td>upgrade ftp-url [--install]</td>
<td>Upgrades the NAM application image.</td>
</tr>
<tr>
<td>ping address</td>
<td>Sends echo messages.</td>
</tr>
<tr>
<td>clear ip</td>
<td>Removes the NAM network configuration.</td>
</tr>
<tr>
<td>clear log upgrade</td>
<td>Clears the log file for the upgrade operation.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>logout</td>
<td>Exits the current session.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the current session.</td>
</tr>
<tr>
<td>passwd-guest</td>
<td>Sets the password for the guest account.</td>
</tr>
<tr>
<td>enable-guest</td>
<td>Enables the guest account.</td>
</tr>
<tr>
<td>disable-guest</td>
<td>Disables the guest account.</td>
</tr>
<tr>
<td>reset</td>
<td>Reboots the NAM (available in guest account only).</td>
</tr>
<tr>
<td>upgrade-bios</td>
<td>Installs a new BIOS image (available in guest account only).</td>
</tr>
</tbody>
</table>
# Appendix B
## Acronyms

Table B-1 defines the acronyms used in this publication.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>ART</td>
<td>Application Response Time</td>
</tr>
<tr>
<td>CDB</td>
<td>circular data base, proprietary NAM database</td>
</tr>
<tr>
<td>CIR</td>
<td>committed information rate</td>
</tr>
<tr>
<td>CLI</td>
<td>command-line interface</td>
</tr>
<tr>
<td>DIFFSERV</td>
<td>differentiated services</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSCP</td>
<td>differentiated services code point</td>
</tr>
<tr>
<td>DSMON</td>
<td>Differentiated Services Monitoring</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization of Standardization</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical unit number. A LUN results from mapping a SCSI logical unit number, port ID, and LDEV ID to a RAID group.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MD5</td>
<td>message digest 5</td>
</tr>
<tr>
<td>MFD</td>
<td>multicast fast drop</td>
</tr>
<tr>
<td>MGCP</td>
<td>Media Gateway Control Protocol</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MII</td>
<td>media-independent interface</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MTU</td>
<td>maximum transmission unit</td>
</tr>
<tr>
<td>NAM</td>
<td>Network Analysis Module</td>
</tr>
<tr>
<td>NDE</td>
<td>NetFlow Data Export</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Network Basic Input/Output System</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer (formerly PCMCIA)</td>
</tr>
<tr>
<td>PHY</td>
<td>physical sublayer</td>
</tr>
<tr>
<td>PTP</td>
<td>Precision Time Protocol (1588)</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RCP</td>
<td>Remote Copy Protocol</td>
</tr>
<tr>
<td>RMON</td>
<td>remote network monitor</td>
</tr>
<tr>
<td>RPC</td>
<td>remote procedure call</td>
</tr>
<tr>
<td>RSPAN</td>
<td>remote SPAN</td>
</tr>
<tr>
<td>SCP</td>
<td>Switch-Module Configuration Protocol</td>
</tr>
<tr>
<td>SCCP</td>
<td>Skinny Client Control Protocol</td>
</tr>
<tr>
<td>SM-SRE</td>
<td>Service Module-Services Ready Engine</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SPAN</td>
<td>Switched Port Analyzer</td>
</tr>
<tr>
<td>SRE</td>
<td>Services Ready Engine</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SVC</td>
<td>switched virtual circuit</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System Plus</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TOS</td>
<td>type of service</td>
</tr>
<tr>
<td>TTL</td>
<td>Time To Live</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>VACL</td>
<td>VLAN access control list</td>
</tr>
<tr>
<td>VLAN</td>
<td>virtual LAN</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VTP</td>
<td>VLAN Trunking Protocol</td>
</tr>
<tr>
<td>WAAS</td>
<td>Wide Area Application Services</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
</tbody>
</table>