



## **Cisco Network Module Enhanced Application Performance Assurance (NME- APA)**

### **CLI Command Reference**

Version 1.0.0  
OL-14500-01

**Corporate 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: 408 526-4100

Customer Order Number: DOC-14500-01=  
Text Part Number: OL-14500-01



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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.-

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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.

CCSP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document 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. (0609R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

*Cisco NME-APA CLI Command Reference*

Copyright © 2002-2007 Cisco Systems, Inc.  
All rights reserved.



## **Preface ix**

- Document Revision History ix
- Audience ix
- Organization x
- Related Publications x
- Conventions x
- Obtaining Documentation xi
  - World Wide Web xi
  - Documentation CD-ROM xi
  - Ordering Documentation xi
  - Documentation Feedback xii
- Obtaining Technical Assistance xii
  - Cisco.com xii
  - Technical Assistance Center xiii

## **Command-Line Interface 1-1**

- Getting Help 1-1
- Authorization and Command Levels (Hierarchy) 1-2
  - CLI Command Hierarchy 1-3
  - CLI Authorization Levels 1-5
  - Prompt Indications 1-7
  - Exiting Modes 1-7
- Navigating Between Configuration Modes 1-8
  - Entering and Exiting Global Configuration Mode 1-8
  - Interface Configuration Modes 1-9
- CLI Help Features 1-11
  - Partial Help 1-11
  - Argument Help 1-12
  - The [no] Prefix 1-12

Navigational and Shortcut Features 1-13

Command History 1-13

Keyboard Shortcuts 1-13

Tab Completion 1-14

FTP User Name and Password 1-14

Managing Command Output 1-15

Scrolling the Screen Display 1-15

Filtering Command Output 1-15

Redirecting Command Output to a File 1-16

CLI Scripts 1-16

**CLI Command Reference 2-1**

Syntax and Conventions 2-1

CLI Commands 2-2

? 2-2

aaa accounting commands 2-3

aaa authentication attempts 2-4

aaa authentication enable default 2-5

aaa authentication login default 2-7

application slot replace force completion 2-8

attack-detector default 2-9

attack-detector 2-11

attack-detector <number> 2-12

attack-detector tcp-port-list|udp-port-list 2-15

attack-filter (Linecard Interface Configuration) 2-16

attack-filter (Privileged Exec) 2-18

attack-filter user-notification ports 2-20

bandwidth 2-21

calendar set 2-22

cd 2-23

clear arp-cache 2-24

clear interface linecard 2-25

clear interface linecard traffic-counter 2-26

clear interface linecard user 2-27

clear interface linecard user db counters 2-28  
clear logger 2-29  
clear management-agent notifications counters 2-31  
clear rdr-formatter 2-32  
clock read-calendar 2-33  
clock set 2-34  
clock summertime 2-35  
clock timezone 2-39  
clock update-calendar 2-40  
configure 2-41  
copy 2-42  
copy ftp:// 2-43  
copy-passive 2-44  
copy running-config startup-config 2-45  
copy source-file ftp:// 2-46  
copy source-file startup-config 2-47  
copy startup-config destination-file 2-48  
default user template all 2-49  
delete 2-50  
dir 2-51  
disable 2-52  
do 2-53  
enable 2-54  
enable password 2-55  
erase startup-config-all 2-56  
exit 2-57  
failure-recovery operation-mode 2-59  
force failure-condition 2-60  
help 2-61  
history 2-63  
history size 2-64  
hostname 2-65  
interface fastethernet 2-66  
interface linecard 2-67

- ip advertising 2-68
- ip domain-lookup 2-70
- ip domain-name 2-71
- ip filter fragment 2-72
- ip filter monitor 2-73
- ip ftp password 2-75
- ip ftp username 2-76
- ip host 2-77
- ip name-server 2-78
- ip radius-client retry limit 2-79
- ip rpc-adapter 2-80
- ip rpc-adapter port 2-81
- ip rpc-adaptor security-level 2-82
- line vty 2-83
- link mode 2-84
- logger add-user-message 2-86
- logger device 2-87
- logger device user-file-log max-file-size 2-88
- logger get support-file 2-89
- logger get user-log file-name 2-90
- logout 2-91
- management-agent sce-api logging 2-92
- management-agent sce-api timeout 2-93
- management-agent system 2-94
- mkdir 2-95
- more 2-96
- more user-log 2-98
- no user 2-99
- no user anonymous-group 2-100
- no user mappings included-in 2-101
- ping 2-102
- pqi install file 2-103
- pqi rollback file 2-104
- pqi uninstall file 2-105

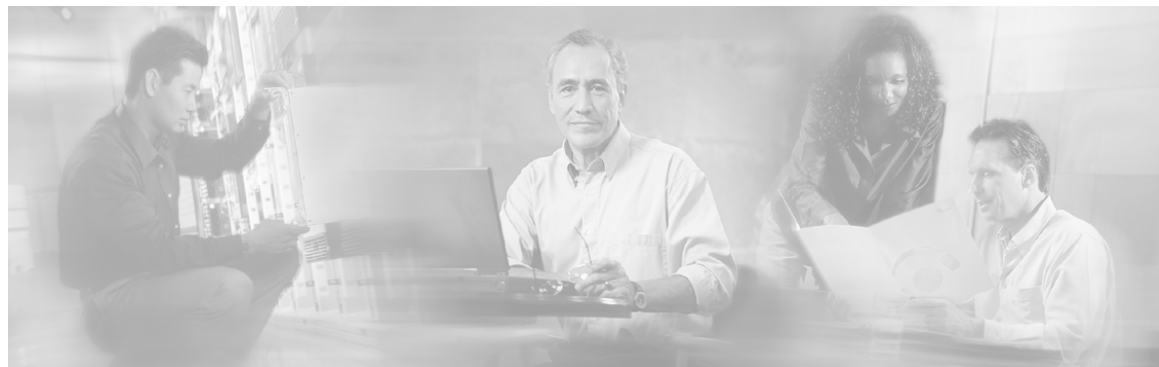
pqi upgrade file 2-106  
pwd 2-107  
queue 2-108  
rdr-formatter category-number 2-109  
rdr-formatter destination 2-110  
rdr-formatter forwarding-mode 2-112  
rdr-formatter history-size 2-113  
rdr-formatter rdr-mapping 2-114  
reload 2-116  
rename 2-117  
rmdir 2-118  
script capture 2-119  
script print 2-120  
script run 2-121  
script stop 2-122  
service password-encryption 2-123  
service rdr-formatter 2-124  
service telnetd 2-125  
setup 2-126  
show calendar 2-129  
show clock 2-130  
show failure-recovery operation-mode 2-131  
show hostname 2-132  
show hosts 2-133  
show interface fastethernet 2-134  
show interface linecard 2-137  
show interface linecard application 2-138  
show interface linecard attack-detector 2-139  
show interface linecard attack-filter 2-144  
show interface linecard counters 2-146  
show interface linecard duplicate-packets-mode 2-147  
show interface linecard flow-open-mode 2-148  
show interface linecard link mode 2-149  
show interface linecard link-to-port-mappings 2-150

show interface linecard shutdown 2-151  
show interface linecard silent 2-152  
show interface linecard tos-marking table 2-153  
show interface linecard traffic-counter 2-154  
show interface linecard traffic-rule 2-155  
show interface linecard user 2-156  
show interface linecard user aging 2-158  
show interface linecard user anonymous 2-159  
show interface linecard user anonymous-group 2-160  
show interface linecard user db counters 2-161  
show interface linecard user mapping 2-163  
show interface linecard user name 2-165  
show interface linecard user properties 2-166  
show interface linecard user templates 2-168  
show inventory 2-169  
show ip advertising 2-170  
show ip filter 2-171  
show ip radius-client 2-173  
show ip rpc-adapter 2-174  
show line vty 2-175  
show log 2-176  
show logger device 2-177  
show pqi file 2-179  
show pqi last-installed 2-180  
show rdr-formatter 2-181  
show rdr-formatter connection-status 2-182  
show rdr-formatter counters 2-183  
show rdr-formatter destination 2-184  
show rdr-formatter enabled 2-185  
show rdr-formatter forwarding-mode 2-186  
show rdr-formatter history-size 2-187  
show rdr-formatter rdr-mapping 2-188  
show rdr-formatter statistics 2-190  
show running-config 2-192

show snmp 2-194  
show snmp community 2-198  
show snmp contact 2-199  
show snmp enabled 2-200  
show snmp host 2-201  
show snmp location 2-202  
show snmp mib 2-203  
show snmp traps 2-205  
show snmp 2-206  
show startup-config 2-207  
show system operation-status 2-208  
show system-uptime 2-209  
show tacacs 2-210  
show telnet sessions 2-212  
show telnet status 2-213  
show timezone 2-214  
show users 2-215  
show version 2-216  
show version all 2-218  
show version software 2-220  
silent 2-221  
snmp-server 2-222  
snmp-server community 2-223  
snmp-server contact 2-224  
snmp-server enable traps 2-225  
snmp-server host 2-227  
snmp-server location 2-228  
snmp broadcast client 2-229  
snmp server 2-230  
snmp update-interval 2-231  
tacacs-server host 2-232  
tacacs-server key 2-234  
tacacs-server timeout 2-235  
telnet 2-236

timeout 2-237  
tos-marking reset-table 2-238  
tos-marking set-table-entry 2-239  
tracert 2-240  
traffic-counter 2-241  
traffic-rule 2-243  
unzip 2-246  
user anonymous-group export csv-file 2-247  
user anonymous-group import csv-file 2-248  
user export csv-file 2-249  
user import csv-file 2-250  
user name property 2-251  
user template export csv-file 2-253  
user template import csv-file 2-254  
user aging 2-255  
username 2-256

**Index 1**



## Preface

---

This guide contains Command-Line Interface (CLI) commands to maintain the NME-APA module. This guide assumes a basic familiarity with telecommunications equipment and installation procedures.

This reference provides a complete listing of all commands at the **admin** authorization level or below, with examples of how to use each command to perform typical NME-APA module management functions.

## Document Revision History

Cisco Service Control Release	Part Number	Publication Date
Release 1.0.0	OL-14500-01	August, 2007

### DESCRIPTION OF CHANGES

This is the first version of this document.

## Audience

This guide is intended for the networking or computer technician responsible for configuring and maintaining the NME-APA module on-site. It is also intended for the operator who manages the NME-APA module. This guide does not cover high-level technical support procedures available to Root administrators and Cisco technical support personnel.

## Organization

This guide covers the following topics:

Chapter	Title	Description
Chapter 1	<i>Command Line Interface</i> (on page 1-1)	Describes how to use the NME-APA module Command-Line Interface (CLI), its hierarchical structure, authorization levels and its help features.
Chapter 2	<i>CLI Command Reference</i> (on page 2-1)	Provides an alphabetical list of the available CLI commands that you can use to configure the NME-APA module.

## Related Publications

This *Cisco Network Module Enhanced-Application Performance Assurance (NME-APA) CLI Command Reference* should be used in conjunction with the following NME-APA manuals to provide a detailed explanation of the commands:

- *Cisco Network Module Enhanced-Application Performance Assurance (NME-APA) Device Console User Guide*

## Conventions

This document uses the following conventions:

Convention	Description
<b>boldface</b> font	Commands and keywords are in <b>boldface</b> .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{x   y   z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x   y   z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
screen font	Terminal sessions and information that the system displays are in screen font.
<b>boldface screen</b> font	Information you must enter is in <b>boldface screen</b> font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> font.

Convention	Description
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not covered in this manual.

**Caution**

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

**Warning**

Means *reader be warned*. In this situation, you might do something that could result in bodily injury.

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package that ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

### Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/cgi-bin/marketplace/welcome.pl>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides [Cisco.com](http://www.cisco.com) (on page [xii](#)) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

### Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to <http://www.cisco.com>.

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website <http://www.cisco.com/tac>.

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for [Cisco.com](http://www.cisco.com) (on page [xii](#)), go to <http://tools.cisco.com/RPF/register/register.do>.

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at <http://www.cisco.com/tac/caseopen>.

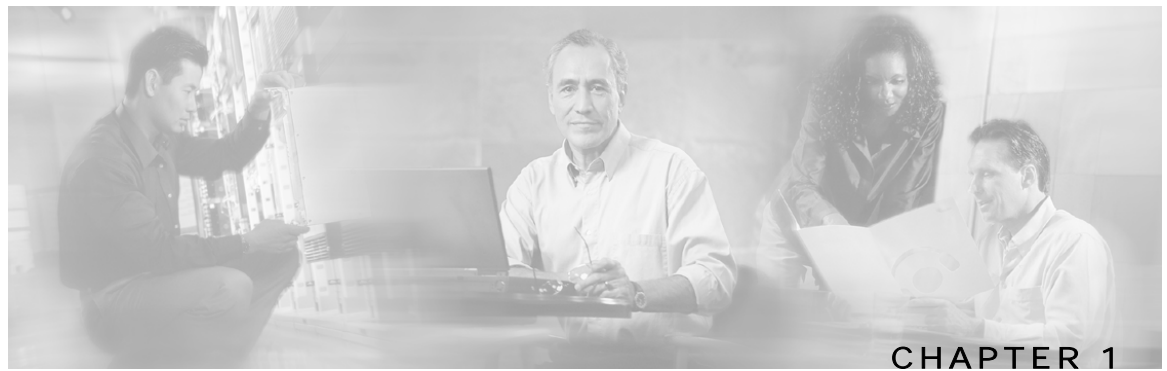
### Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.





# Command-Line Interface

---

This chapter describes how to use the NME-APA module Command-Line Interface (CLI), its hierarchical structure, authorization levels and its help features. The Command-Line Interface is one of the NME-APA module management interfaces.

This chapter contains the following sections:

- [Getting Help](#) 1-1
- [Authorization and Command Levels \(Hierarchy\)](#) 1-2
- [Navigating Between Configuration Modes](#) 1-8
- [CLI Help Features](#) 1-11
- [Navigational and Shortcut Features](#) 1-13
- [Managing Command Output](#) 1-15
- [CLI Scripts](#) 1-16

The CLI is accessed through a Telnet session. When you enter a Telnet session, you enter as the simplest level of user, in the User Exec mode.

The NME-APA module supports up to five concurrent CLI sessions.

## Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark (?) at the system prompt. You also can obtain a list of keywords and arguments associated with any command using the context-sensitive help feature.

The following table lists commands you can enter to get help that is specific to a command mode, a command, a keyword, or an argument.

Table 1-1 Getting Help

Command	Purpose
abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
abbreviated-command-entry<Tab>	Complete a partial command name.
?	List all commands available for a particular command mode.
command ?	List the keywords associated with the specified command.  Leave a space between the command and question mark.
command keyword ?	List the arguments associated with the specified keyword.  Leave a space between the keyword and question mark.

## Authorization and Command Levels (Hierarchy)

When using the CLI there are two important concepts that you must understand in order to navigate:

- **Authorization Level** — Indicates the level of commands you can execute. A user with a simple authorization level can only view some information in the system, while a higher level administrator can actually make changes to configuration.

This manual documents commands at the User, Viewer, and Admin authorization levels. See [CLI Authorization Levels](#) (on page 1-5).

- **Command Hierarchy Level** — Provides you with a context for initiating commands. Commands are broken down into categories and you can only execute each command within the context of its category. For example, in order to configure parameters related to the Line Card, you need to be within the LineCard Interface Configuration Mode. See [CLI Command Hierarchy](#) (on page 1-3).

The following sections describe the available Authorization and Command Hierarchy Levels and how to maneuver within them.

The on-screen prompt indicates both your authorization level and your command hierarchy level, as well as the assigned host name. See [Prompt Indications](#) (on page 1-7).



### Note

Throughout the manual, *NME-APA* is used as the sample host name.

## CLI Command Hierarchy

The set of all CLI commands is grouped in hierarchical order, according to the type of the commands. The first two levels in the hierarchy are the User Exec and Privileged Exec modes. These are non-configuration modes in which the set of available commands enables the monitoring of the NME-APA module, file system operations, and other operations that cannot alter the configuration of the NME-APA module.

The next levels in the hierarchy are the Global and Interface configuration modes, which hold a set of commands that control the global configuration of the NME-APA module and its interfaces. Any of the parameters set by the commands in these modes should be saved in the startup configuration, such that in the case of a reboot, the NME-APA module restores the saved configuration.

The following table shows the available CLI modes.

Table 1-2 CLI Modes

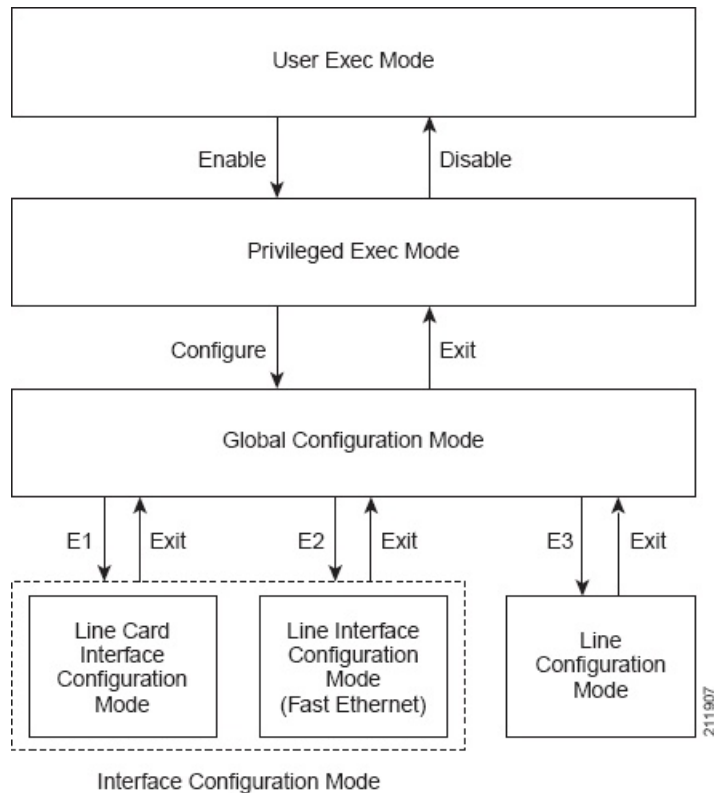
Mode	Description	Level	Prompt indication
<b>User Exec</b>	Initial mode with very limited functionality.	User/ Viewer	<i>NME-APA</i> >
<b>Privileged Exec</b>	General administration; file system manipulations and control of basic parameters that do not change the configuration of the NME-APA module.	Admin	<i>NME-APA</i> #
<b>Global Configuration</b>	Configuration of general system parameters, such as DNS, host name, and time zone.	Admin	<i>NME-APA</i> (config)#
<b>Interface Configuration</b>	Configuration of specific system interface parameters, such as the Line Card, and the Ethernet interfaces.	Admin	<i>NME-APA</i> (config if)#
<b>Line Configuration</b>	Configuration of Telnet lines.	Admin	<i>NME-APA</i> (config-line)#

When you login to the system, you have the User authorization level and enter User Exec mode. Changing the authorization level to Viewer does not change the mode. Changing the authorization level to Admin automatically moves you to Privileged Exec mode. In order to move to any of the configuration modes, you must enter commands specific to that mode.

The list of available commands in each mode can be viewed using the question mark '?' at the end of the prompt.

The figure below, illustrates the hierarchical structure of the CLI modes, and the CLI commands used to enter and exit a mode.

Figure 1-1: CLI Command Hierarchy



The following commands are used to enter the different configure interface modes and the Line Configuration Mode:

- E1 **interface LineCard 0**
- E2 **interface FastEthernet 0/1 or 0/2** (line ports, NME-APA module)
- E3 **line vty 0**



**Note**

Although the system supports up to five concurrent Telnet connections, you cannot configure them separately. This means that any number you enter in the **line vty** command (**0, 1, 2, 3** or **4**) will act as a **0** and configure all five connections together.



**Note**

In order for the auto-completion feature to work, when you move from one interface configuration mode to another, you must first exit the current interface configuration mode (as illustrated in the above figure).

**EXAMPLE:**

This example illustrates moving into and out of configuration modes as follows:

- Enter global configuration mode
- Configure the NME-APA module time zone
- Enter the LineCard Interface configuration
- Define the link mode.
- Exit LineCard Interface configuration mode to the global configuration mode
- Exit global configuration mode

```
NME-APA#configure
NME-APA(config)#clock timezone PST -10
NME-APA(config)#interface LineCard 0
NME-APA(config if)#link-mode port1-port2 forwarding
NME-APA(config if)#exit
NME-APA(config)#exit
NME-APA#
```

## CLI Authorization Levels

The NME-APA module has four authorization levels, which represent the user access permissions. When you initially connect to the NME-APA module, you automatically have the most basic authorization level, that is User, which allows minimum functionality.

In order to monitor the system, you must have Viewer authorization, while in order to perform administrative functions on the NME-APA module, you must have Admin or Root authorization. A higher level of authorization is accessed by logging in with appropriate password, as described in the procedures below.

In each authorization level, all the commands of the lower authorization layers are available in addition to commands that are authorized only to the current level.

**Note**

This manual covers the functions that can be performed by the Admin level user, unless otherwise noted.

The following CLI commands are related to authorization levels:

- enable
- disable

Each authorization level has a value (number) corresponding to it. When using the CLI commands, use the values, not the name of the level, as shown in the following table.

Table 1-3 Authorization Levels

Level	Description	Value	Prompt
User	Password required. This level enables basic operational functionality.	0	>
Viewer	Password required. This level enables monitoring functionality. All show commands are available to the Viewer authorization level, with the exception of those that display password information.	5	>
Admin	Password required. For use by general administrators, the Admin authorization level enables configuration and management of the NME-APA module.	10	#
Root	Password required. For use by technical field engineers, the Root authorization level enables configuration of all advanced settings, such as debug and disaster recovery. The Root level is used by technical engineers only and is not documented in this manual.	15	#>

To change from User to Viewer level authorization:

---

**Step 1** From the *NME-APA*> prompt, type **enable 5** and press **Enter**.

The system prompts for a password by showing the prompt *Password*:

**Step 2** Type in the password for the Viewer level and press **Enter**.

Note that the password is an access-level authorization setting, not an individual user password.

The system prompt *NME-APA*> does not change when you move from User to Viewer level.

---

A telnet session begins with a request for password, and will not continue until the proper user password is supplied. This enhances the security of the system by not revealing its identity to unauthorized people.

To log in with Admin level authorization:

---

**Step 1** Initiate a telnet connection.

**Step 2** A *Password*: prompt appears. Type in the user level password and press **Enter**.

The *NME-APA*> prompt appears.

You now have user level authorization.

**Step 3** From the *NME-APA*> prompt, type **enable 10** and press **Enter**.

The system prompts for a password by showing the prompt *Password*:

**Step 4** Type in the password for the Admin level and press **Enter**.

Note that the password is an access-level authorization setting, not an individual user password.

The system prompt changes to *NME-APA#* to show you are now in Admin level.

#### EXAMPLE:

The following example illustrates how to change the authorization level from User to Admin, and then revert back to Viewer. No password is required for moving to a lower authorization level.

```
NME-APA>enable 10
Password: cisco
NME-APA#disable
NME-APA>
```

## Prompt Indications

The on-screen prompt indicates your authorization level, your command hierarchy level, and the assigned host name. The structure of the prompt is:

```
<hostname(mode-indication)level-indication>
```

Authorization levels are indicated as follows:

This prompt...	Indicates this...
>	indicates User and Viewer levels
#	indicates Admin level
#>	indicates Root level

Command hierarchy levels are indicated as follows:

This command hierarchy...	Is indicated as...
User Exec	<i>NME-APA</i> >
Privileged Exec	<i>NME-APA</i> #
Global Configuration	<i>NME-APA</i> (config)#
Interface Configuration	<i>NME-APA</i> (config if)#
Line Configuration	<i>NME-APA</i> (config-line)#

#### EXAMPLE:

The prompt *NME-APA1(config if)#* indicates:

- The name of the NME-APA module is *NME-APA1*
- The current CLI mode is Interface configuration mode
- The user has Admin authorization level

## Exiting Modes

This section describes how to revert to a previous mode.

- To exit from one authorization level to the previous one, use the **disable** command.
- To exit from one mode to another with the Admin authorization level (these are the various configuration modes), use the **exit** command.

To exit from the Privileged Exec mode and revert to the Viewer mode:

---

At the *NME-APA*# prompt, type **disable**, and press **Enter**.

The *NME-APA*> prompt for the Viewer and User Exec mode appears.

---

To exit from the Global Configuration Mode:

---

At the *NME-APA* (config)# prompt, type **exit**, and press **Enter**.

The appropriate prompt for the previous level appears.

---

#### EXAMPLE:

The following example shows the system response when you exit the Interface Configuration mode.

```
NME-APA(config if)#exit  
NME-APA(config)#
```

## Navigating Between Configuration Modes

### Entering and Exiting Global Configuration Mode

To enter the Global Configuration Mode:

---

At the *NME-APA*# prompt, type **configure**, and press **Enter**.

The *NME-APA*(config)# prompt appears.

---

To exit the Global Configuration Mode:

---

At the *NME-APA*(config)# prompt, type **exit** and press **Enter**.

The *NME-APA*# prompt appears.

---

## Interface Configuration Modes

The components that are configured by the Interface Configuration Modes are:

- Card
  - LineCard — **Interface LineCard 0**  
The LineCard interface configures the main functionality of viewing and handling traffic on the line.
- Ports
  - See [Configuring the Physical Ports](#) (on page 1-9)
- Telnet
  - Line Configuration Mode — **Line vty 0**  
The Line Configuration Mode enables you to configure Telnet parameters.

### Configuring the Physical Ports

The NME-APA module contains the following physical port interfaces:

- Fast Ethernet:

**Interface FastEthernet 0/1 or 0/2**

The FastEthernet Interface mode configures the settings for the FastEthernet interface to the Internet traffic on the wire. Each of the two ports can be set individually.

The following commands are used to configure the Fast Ethernet line ports:

- bandwidth
- queue



---

**Note**

You must specify the slot number/interface number when referencing any interface. The slot number is always 0, and the interfaces are numbered as follows:  
Fast Ethernet Line Interfaces: 1,2

---

### Entering LineCard Interface Configuration Mode

The following procedure is for entering Line Card Interface Configuration mode. The procedures for entering the other interfaces are the same except for the interface command as described above and in [CLI Command Reference](#) (on page 2-1).

To enter LineCard Interface Configuration mode:

- 
- Step 1** To enter Global Configuration Mode, at the *NME-APA*# prompt, type **configure**, and press **Enter**.

The *NME-APA* (config)# prompt appears.

**Step 2** Type **interface LineCard 0**, and press **Enter**.

The *NME-APA*(config if)# prompt appears.

**Step 3** To return to Global Configuration Mode, type **exit** and press **Enter**.

The *NME-APA*(config)# prompt appears.

**Step 4** To exit Global Configuration Mode, type **exit** and press **Enter**.

The *NME-APA*# prompt appears.

---

## Entering the Fast Ethernet Line Interface Configuration Mode

To enter the FastEthernet Interface Configuration Mode:

---

**Step 1** To enter Global Configuration Mode, type **configure** and press **Enter**.

The *NME-APA*(config)# prompt appears.

**Step 2** Type **interface FastEthernet [0/1|0/2]** and press **Enter**.

The *NME-APA*(config if)# prompt appears.

---

### EXAMPLE:

The following example shows how to enter Configuration Mode for the FastEthernet Interface number 1.

```
NME-APA(config)#interface FastEthernet 0/1
NME-APA(config if)#
```

## Navigating between the Interface Configuration Modes

To navigate from one Interface Configuration Mode to another:

---

**Step 1** Type **exit**.

You are returned to the Global Configuration Mode.

**Step 2** Type the appropriate command to enter a different Interface Configuration Mode.

---

## The "do" Command: Executing Commands Without Exiting

There are three configuration command modes:

- Global configuration mode
- Interface configuration mode
- Line configuration mode

When you are in one of these configuration modes, it is possible to execute an EXEC mode command (such as a show command) or a privileged EXEC (such as **show running-config**) without exiting to the relevant command mode. Use the 'do' command for this purpose.

To execute an exec mode command from a configuration command mode, use the following command:

---

```
At the NME-APAconfig# (or NME-APAconfig if#) prompt, type do <command>.
```

```
The specified command executes without exiting to the appropriate exec command mode.
```

---

### EXAMPLE

The following example shows how to display the running configuration while in interface configuration mode.

```
NME-APAconfig if# do show running-config
```

## CLI Help Features

CLI provides context sensitive help. Two types of context sensitive help are supported:

- Partial help
- Argument help

### Partial Help

To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called partial help, because it lists only the keywords or arguments that begin with the abbreviation you entered.

#### EXAMPLE:

The following example illustrates how typing **c?** displays all available arguments that start with the letter c.

```
NME-APA(config)#snmp-server c?  
Community          contact  
NME-APA(config)#snmp-server c
```

## Argument Help

To obtain a list of command's associated keywords or parameters, type a question mark (?) in place of a keyword or parameter on the command line.

Note that if <Enter> is acceptable input, the symbol <cr> represents the **Enter** key.

### EXAMPLE:

The following example illustrates how to get a list of all arguments or keywords expected after the command **snmp-server**.

```
NME-APA(config)#snmp-server ?
Community   Define community string
Contact     Set system contact
Enable      Enable the SNMP agent
Host        Set traps destination
Interface   Set interface parameters
Location    Set system location
NME-APA(config)# snmp-server
```

When asking for help on a particular parameter, the system informs you of the type of data that is an accepted legal value. The types of parameters supported are:

**STRING** When a String is expected, you can enter any set of characters or digits. If the string has a space as one of its characters, use double-quote (") marks to enclose the string.

**DECIMAL** Any decimal number. Positive number is assumed, for negative numbers use the "-" symbol.

**HEX** A hexadecimal number; must start with either 0x or 0X.

### EXAMPLE:

The following example illustrates the use of ? to get help on commands syntax. In this example, you can enter either the word **running-config**, or any name of a file, after the word **copy**.

```
NME-APA#copy ?
  running-config      Copy running configuration file
  running-config-all  Copy all running configuration files
  running-config-application  Copy running application
  configuration file
  startup-config      Backup the startup-config to a
  specified destination
  STRING              Source file name
NME-APA#copy
```

## The [no] Prefix

Many CLI commands offer the option of adding the word **no** before the command to disable the feature controlled by the command or revert it to its default configuration. This notation is shown in the *CLI Command Reference* (on page 2-1) as **[no]** to denote it is optional.

For example, **no service telnetd** disables the telnet server. Enabling the telnet server is done by typing **service telnetd**.

# Navigational and Shortcut Features

## Command History

CLI maintains a history buffer of the most recent commands you used in the current CLI session for quick retrieval. Using the keyboard, you can navigate through your last commands, one by one, or all commands that start with a given prefix. By default, the system saves the last 30 commands you typed. You can change the number of commands remembered using the **history size** command.

To use the history functions, use the keys shown in the following table.

**Table 1-4 Keyboard Shortcuts for History Functions**

Arrow	Shortcut	Description
Up arrow	Ctrl-P	Moves cursor to the previous command with the same prefix.
Down arrow	Ctrl-N	Moves cursor to the next command with the same prefix as original.
	Ctrl-L Ctrl-R	Re-display the current command line.

## Keyboard Shortcuts

The NME-APA module has a number of keyboard shortcuts that make it easier to navigate and use the system. The following table shows the keyboard shortcuts available.

You can get a display the keyboard shortcuts at any time by typing **help bindings**.

**Table 1-5 Keyboard Shortcuts**

Description	Shortcut Key
<b>Navigational shortcuts</b>	
Move cursor one character to the right.	CTRL-F /->
Move cursor one character to the left.	CTRL-B /<-
Move cursor one word to the right (forward).	ESC-F
Move cursor one word to the left (backward).	ESC-B
Move cursor to the start of the line.	CTRL-A
Move cursor to the end of the line.	CTRL-E
<b>Editing shortcuts</b>	
Delete the character where the cursor is located.	CTRL-D
Delete from the cursor position to the end of the word.	ESC-d
Delete the character before the current location of the cursor.	Backspace
Delete the character before the current location of the cursor.	CTRL-H
Deletes from the cursor position to the end of the line	CTRL-K

Description	Shortcut Key
Deletes all characters from the cursor to the beginning of the line	CTRL-U
Deletes all characters from the cursor to the beginning of the line. (Same functionality as CTRL-U.)	CTRL-X
Delete the word to the left of the cursor.	CTRL-W
Recall the last item deleted.	CTRL-Y
Completes the word when there is only one possible completion.	<Tab>
Completes the word when there is only one possible completion. (Same functionality as <Tab>.)	CTRL-I

## Tab Completion

The CLI interface features tab completion. When you type in the first letters of a command and type <Tab>, the system automatically fills in the rest of the command or keyword. This feature works only when there is one possible command that could be possible using the starting letters.

### EXAMPLE:

The letters **snm** followed by <Tab> will be completed to the command **snmp-server**.

```
NME-APA(config)#snm<Tab>
NME-APA(config)#snmp-server
```

If you type <Enter> instead of <Tab>, and there is no ambiguity, the system actually carries out the command which would be filled in by the rest of the word.

### EXAMPLE:

The following example displays how the system completes a partial (unique) command for the **enable** command. Because **enable** does not require any parameters, the system simply carries out the **enable** command when the user presses **Enter**.

```
NME-APA>en<Enter>
Password:
NME-APA#
```

## FTP User Name and Password

CLI enables saving ftp user name and password to be used in FTP operations—download and upload, per session.

These settings are effective during the current CLI session.

### EXAMPLE:

The following example illustrates how to set FTP password and user name and the use in these settings for getting a file named *config.tmp* from a remote station using FTP protocol.

```
NME-APA#ip ftp password vk
NME-APA#ip ftp username vk
NME-APA#copy ftp://@10.1.1.253/h:/config.tmp myconf.txt
connecting 10.1.1.253 (user name vk password vk) to retrieve
config.tmp
NME-APA#
```

# Managing Command Output

Some commands, such as many **show** commands, may have many lines of output. There are several ways of managing the command output:

- Scrolling options — When the command output is too large to be displayed all at once, you can control whether the display scrolls line by line or refreshes the entire screen.
- Filtering options — You can filter the output so that output lines are displayed only if they include or exclude a specified expression.
- Redirecting to a file — You can send the output to a specified file

## Scrolling the Screen Display

The output of some **show** and **dir** commands is quite lengthy and cannot all be displayed on the screen at one time. Commands with many lines of output are displayed in chunks of 24 lines. You can choose to scroll the display line by line or refresh the entire screen. At the prompt after any line, you can type one of the following keys for the desired action:

- **<Enter>**— show one more line
- **<Space>** – show 24 more lines (a new chunk)
- **<g>** – Stop prompting for more
- **<?>** – Display a help string showing possible options
- Any other key – quit showing the file

## Filtering Command Output

You can filter the output of certain commands, such as **show**, **more**, and **dir**, so that output lines are displayed only if they include or exclude a specified expression. The filtering options are as follows:

- **include** — Shows all lines that include the specified text.
- **exclude** — Does not show any lines that include the specified text.
- **begin** — Finds the first line that includes the specified text, and shows all lines starting from that line. All previous lines are excluded.

The syntax of filtered commands is as follows:

- **<command> | include <expression>**
- **<command> | exclude <expression>**
- **<command> | begin <expression>**

The **<expression>** in these commands is case sensitive.

### EXAMPLE

Following is an example of how to filter the **show version** command to display only the last part of the output, beginning with the version information.

```
NME-APA# show version | include version
```

## Redirecting Command Output to a File

You can redirect the output of commands, such as **show**, **more**, and **dir**, to a file. When writing the output of these commands to a file, you can specify either of the following options:

- **redirect** — The new output of the command will overwrite the existing contents of the file.
- **append** — The new output of the command will be appended to the existing contents of the file.

The syntax of redirection commands is as follows:

- `<command> | redirect <file-name>`
- `<command> | append <file-name>`

### EXAMPLE

Following is an example of how to do the following:

- Filter the **more** command to display from a *csv user* file only the gold package users.
  - Redirect that output to a file named *current\_gold\_users*. The output should not overwrite existing entries in the file, but should be appended to the end of the file.
- ```
NME-APA# more users_10.10.2004 | include gold append
current_gold_users
```

## CLI Scripts

The CLI scripts feature allows you to record several CLI commands together as a script and play it back. This is useful for saving repeatable sequence of commands, such as software upgrade. For example, if you are configuring a group of NME-APA modules and you want to run the same configuration commands on each platform, you could create a script on one platform and run it on all the other NME-APA modules.

The available script commands are:

- `script capture`
- `script stop`
- `script print`
- `script run`

To create a script:

- 
- Step 1** At the *NME-APA#* prompt, type **script capture** *sample1.scr* where *sample1.scr* is the name of the script.
- Step 2** Perform the actions you want to be included in the script.
- Step 3** Type **script stop**.
- The system saves the script.
-

**EXAMPLE:**

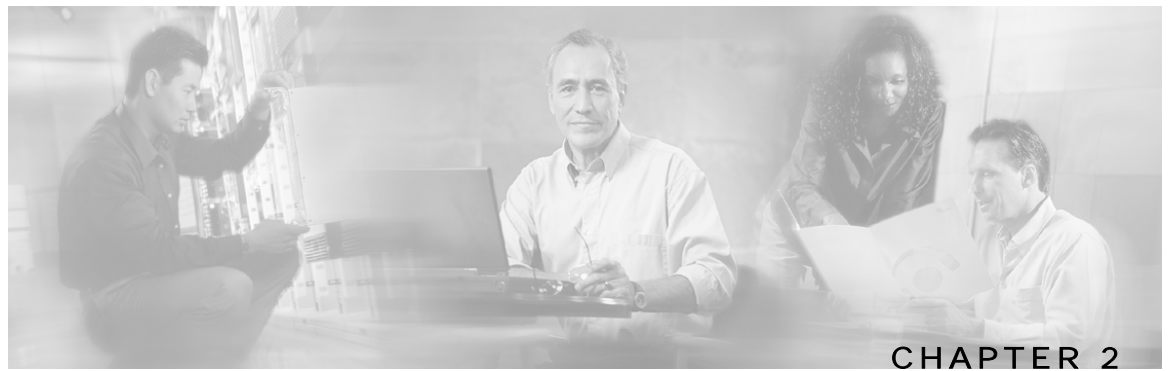
The following is an example of recording a script for defining users.

```
NME-APA#script capture users.scr  
NME-APA#configure  
NME-APA(config)#username John privilege 15 password BfgVxsm  
NME-APA(config)#username Kathy privilege 10 password Muiyop  
NME-APA(config)#aaa authentication login default local enable  
NME-APA(config)#exit  
NME-APA#copy running-config startup-config  
Writing general configuration file to temporary location...  
Backing-up general configuration file...  
Copy temporary file to final location...  
NME-APA#script stop  
NME-APA#
```

To run the script recorded above, type:

```
NME-APA#script run users.scr
```





# CLI Command Reference

---

This chapter contains all the CLI commands available on the NME-APA module.

Each command description is broken down into the following sub-sections:

|                  |                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command syntax   | The general format of the command.                                                                                                                                    |
| Description      | Description of what the command does.                                                                                                                                 |
| Default          | If relevant, the default setting for the command.                                                                                                                     |
| Authorization    | The level of user authorization required for using the command.                                                                                                       |
| Mode             | The mode (command line) from which the command can be invoked.                                                                                                        |
| Parameters       | Description of parameters and switches for the command.                                                                                                               |
| Usage guidelines | Information about when to invoke the command and additional details.                                                                                                  |
| Example          | An illustration of how the command looks when invoked. Because the interface is straightforward, some of the examples are obvious, but they are included for clarity. |

This chapter contains the following sections:

- [Syntax and Conventions](#) 2-1
- [CLI Commands](#) 2-2

## Syntax and Conventions

The CLI commands are written in the following format:

**command** *required-parameter* [*optional-parameter*]

[no] is an optional parameter that may appear before the command name.

- When typing commands, you may enclose parameters in double-quote marks, and you *must* do so when there is a space within a parameter name.
- Examples are shown in courier style. **Bold courier** is used to show the commands as you type them and regular *courier* is used for system prompts and responses.

# CLI Commands

## ?

Lists all of the commands available for the current command mode. You can also use the ? command to get specific information on a keyword or parameter.

To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called partial help, because it lists only the keywords or arguments that begin with the abbreviation you entered.

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | This command has no arguments or keywords                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Defaults           | This command has no default settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Command Modes      | All                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Usage Guidelines   | <p>To list a command's associated keywords or arguments, enter a question mark (?) in place of a keyword or parameter on the command line. This form of help is called argument help because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.</p> <p>Authorization: User</p>                                                                                                                                                                                                                                                                                                                                                                        |
| Examples           | <p>The following example shows ways of requesting help using the ? wildcard.</p> <pre> <b>NME-APA</b>(config)#ip ? advertising      Enable IP advertising or set parameters domain-lookup    Enables the IP DNS-based host name-to-address translation domain-name      Define a default domain name host              Add a host to the host table name-server       Specify the address of one or more name servers to use for name and address resolution radius-client     RADIUS-Client settings rpc-adapter       Enable PRPC adapter or set attributes <b>NME-APA</b>(config)#ip d? default-gateway  domain-lookup  domain-name <b>NME-APA</b>(config)#ip de? default-gateway <b>NME-APA</b>(config)#ip de </pre> |
| Related Commands   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## aaa accounting commands

Enables TACACS+ accounting.

Use the **no** form of the command to disable TACACS+ accounting.

**aaa accounting commands *level* default stop-start group tacacs+**

**no aaa accounting commands *level* default**

### Syntax Description

*level* The privilege level for which to enable the TACACS+ accounting

0: User

5: Viewer

10: Admin

15: Root

### Defaults

By default, TACACS+ accounting is disabled.

### Command Modes

Global Configuration

### Usage Guidelines

If TACACS+ accounting is enabled, the NME-APA module sends an accounting message to the TACACS+ server after every command execution. The accounting message is logged in the TACACS+ server for the use of the network administrator.

The **start-stop** keyword (required) indicates that the accounting message is sent at the beginning and the end (if the command was successfully executed) of the execution of a CLI command.

Authorization: admin

### Examples

The following example enables TACACS+ accounting for the admin privilege level (10).

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#aaa accounting commands 10 default stop-start  
group tacacs+
```

```
NME-APA(config)#
```

### Related Commands

[aaa authentication attempts](#) (on page 2-4)

[aaa authentication enable default](#) (on page 2-5)

[aaa authentication login default](#) (on page 2-7)

[tacacs-server host](#) (on page 2-232)

[tacacs-server key](#) (on page 2-234)

## aaa authentication attempts

Sets the maximum number of login attempts that will be permitted before a Telnet session is terminated.

**aaa authentication attempts login** *number-of-attempts*

---

|                    |                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>number-of-attempts</i> the maximum number of login attempts that will be permitted before the telnet session is terminated |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|

---



---

|          |                                       |
|----------|---------------------------------------|
| Defaults | Default <i>number-of-attempts</i> = 3 |
|----------|---------------------------------------|

---



---

|               |                      |
|---------------|----------------------|
| Command Modes | Global Configuration |
|---------------|----------------------|

---



---

|                  |                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | The maximum number of login attempts is relevant only for Telnet sessions. From the local console, the number of re-tries is unlimited. |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

Authorization: admin

---

|          |                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Examples | <p>The following example shows how to set the maximum number of logon attempts to five.</p> <pre><b>NME-APA</b>&gt;enable 10 Password:&lt;cisco&gt; <b>NME-APA</b>#config product&gt;(config)# <b>aaa authentication attempts login 5</b> <b>NME-APA</b>(config)#</pre> |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---



---

|                  |                                                                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Related Commands | <p><a href="#">aaa authentication accounting commands</a> (on page 2-3)</p> <p><a href="#">aaa authentication enable default</a> (on page 2-5)</p> <p><a href="#">aaa authentication login default</a> (on page 2-7)</p> |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## aaa authentication enable default

Specifies which privilege level authentication methods are to be used, and in what order of preference.

Use the no form of the command to delete the privilege level authentication methods list.

**aaa authentication enable default** *method1* [*method2...*]

**no aaa authentication enable default**

### Syntax Description

*method* the privilege level authentication methods to be used. You may specify up to four different methods, in the order in which they are to be used

### Defaults

Default privilege level authentication method = **enable** only

### Command Modes

Global Configuration

### Usage Guidelines

Use this command to configure "backup" privilege level authentication methods to be used in the event of failure of the primary privilege level authentication method.

The following method options are available:

- **group tacacs+**: Use TACACS+ authentication.
- **local**: Use the local username database for authentication.
- **enable** (default): Use the "enable" password for authentication
- **none**: Use no authentication.

If the privilege level authentication methods list is deleted, the default privilege level authentication method only (**enable** password) will be used. TACACS+ authentication will not be used.

Authorization: admin

### Example

This example shows how to configure privilege level authentication methods.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)# aaa authentication enable default group tacacs+
enable none
NME-APA(config)#
```

### Related Commands

[aaa authentication login default](#) (on page 2-7)

[aaa authentication accounting commands](#) (on page 2-3)

*aaa authentication attempts* (on page 2-4)

*tacacs-server host* (on page 2-232)

## aaa authentication login default

Specifies which login authentication methods are to be used, and in what order of preference.

Use the no form of the command to delete the login authentication methods list.

**aaa authentication login default** *method1* [*method2...*]

**no aaa authentication login default**

### Syntax Description

*method* the login authentication methods to be used. You may specify up to four different methods, in the order in which they are to be used

### Defaults

Default login authentication method = **enable** only

### Command Modes

Global Configuration

### Usage Guidelines

Use this command to configure "backup" login authentication methods to be used in the event of failure of the primary login authentication method.

The following method options are available:

- **group tacacs+**: Use TACACS+ authentication.
- **local**: Use the local username database for authentication.
- **enable** (default): Use the "enable" password for authentication
- **none**: Use no authentication.

If the login authentication methods list is deleted, the default login authentication method only (**enable** password) will be used. TACACS+ authentication will not be used.

Authorization: admin

### Example

This example shows how to configure login authentication methods.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)# aaa authentication login default group tacacs+
enable none
NME-APA(config)#
```

### Related Commands

[aaa authentication enable default](#) (on page 2-5)

[aaa authentication accounting commands](#) (on page 2-3)

[aaa authentication attempts](#) (on page 2-4)

[tacacs-server host](#) (on page 2-232)

## application slot replace force completion

Forces the current application replace process to complete and immediately start finalization (killing all old flows).

**application slot *slot-number* replace force completion**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example illustrates how to force the application replace operation to complete immediately.

```
NME-APA>enable 10
NME-APA>Password:<cisco>
NME-APA#application slot 0 replace force completion
NME-APA#
```

---

### Related Commands

## attack-detector default

Defines default thresholds and attack handling action. If a specific attack detector is defined for a particular situation (protocol/attack direction/side), it will override these defaults.

Use the **no** version of this command to delete the user-defined defaults. The system defaults will then be used.

**attack-detector default protocol** *protocol* **attack-direction** *attack-direction* **side** *side* [**action** *action*] [**open-flows** *open-flows*] [**ddos-suspected-flows** *ddos-suspected-flows*] [**suspected-flows-ratio** *suspected-flows-ratio*] [**notify-user|dont-notify-user**] [**alarm|no-alarm**]

**no attack-detector default protocol** *protocol* **attack-direction** *attack-direction* **side** *side* [**action** *action*] [**open-flows** *open-flows*] [**ddos-suspected-flows** *ddos-suspected-flows*] [**suspected-flows-ratio** *suspected-flows-ratio*]

---

### Syntax Description

*protocol*     **TCP, UDP, ICMP, other**

*attack-direction* **attack-source, attack-destination, both**

*side*         **user, network, both**

*action*       **report, block** (block is not currently supported.)

*open-flows*    Threshold for concurrently open flows (new open flows per second).

*ddos-suspected-flows*    Threshold for DDoS-suspected flows (new suspected flows per second).

*suspected-flows-ratio*    Threshold for ratio of suspected flow rate to open flow rate.

---



---

### Defaults

The default values for the default attack detector are

- Action = Report
- Thresholds — Varies according to the attack type
- User notification = Disabled
- Sending an SNMP trap = Disabled

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

The following arguments must always be specified:

- protocol
- attack-direction
- side

The following arguments are optional:

- action
- open-flows

- `ddos-suspected-flows`
- `suspected-flows-ratio`

Use the optional keywords as follows:

- Use the `notify-user` keyword to enable subscriber notification. (Use the [\*attack-filter user-notification ports\*](#) (on page 2-20) command to configure the port to be used for user notification.)
- Use the `dont-notify-user` keyword to disable user notification.
- Use the `alarm` keyword to enable sending an SNMP trap.
- Use the `no-alarm` keyword to disable sending an SNMP trap.

Use the [\*attack-detector <number>\*](#) (on page 2-12) command to configure a specific attack detector.

Authorization: admin

## Examples

The following examples illustrate the use of the **attack-detector default** command:

### EXAMPLE 1:

The following example configures a default attack detector for TCP flows from the attack source.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-detector default protocol TCP attack-
direction attack-source side both action report open-flows 500
ddos-suspected-flows 75 suspected-flows-ratio 50
NME-APA(config if)#
```

### EXAMPLE 2:

The following example enables user notification for the specified default attack detector.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-detector default protocol TCP attack-
direction attack-source side both notify-user
NME-APA(config if)#
```

## Related Commands

- [\*attack-detector <number>\*](#) (on page 2-12)
- [\*attack-filter user-notification ports\*](#) (on page 2-20)
- [\*show interface linecard attack-detector\*](#) (on page 2-139)

## attack-detector

Enables the specified attack detector and assigns an access control list (ACL) to it.

**attack-detector** *number*

---

### Syntax Description

---

*number* The attack detector number.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Use the following commands to define the attack detector:

- Attack detector: [attack-detector <number>](#) (on page 2-12)

Authorization: admin

---

### Examples

The following example enables attack detector number "2".

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-detector 2
NME-APA(config if)#
```

[attack-detector <number>](#) (on page 2-12)

---

### Related Commands

[show interface linecard attack-detector](#) (on page 2-139)

**attack-detector <number>**

Configures a specific attack detector for a particular attack type (protocol/attack direction/side) with the assigned number.

Use the **attack-detector default** form of this command to configure the default attack detector for the specified attack type.

Use the **no** form of this command to delete the specified attack detector.

Use the **default attack-detector** form of the command to use the default attack detector configuration for the specified attack detector(s). The *all* and *all-numbered* options also disable all numbered attack detectors.

**attack-detector <number> protocol** (((TCP|UDP) [dest-port (specific|not-specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (user|network|both) [**action** (report|block)] [**open-flows** *open-flows*] [**ddos-suspected-flows** *ddos-suspected-flows*] [**suspected-flows-ratio** *suspected-flows-ratio*] [**notify-user|dont-notify-user**] [**alarm|no-alarm**]

**no attack-detector <number>**

**attack-detector default protocol** (((TCP|UDP) [dest-port (specific|not-specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (user|network|both) [**action** (report|block)] [**open-flows** *open-flows*] [**ddos-suspected-flows** *ddos-suspected-flows*] [**suspected-flows-ratio** *suspected-flows-ratio*] [**notify-user|dont-notify-user**] [**alarm|no-alarm**]

**no attack-detector default protocol** (((TCP|UDP) [dest-port (specific|not-specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (user|network|both)

**default attack-detector** {all |all-numbered }

**default attack-detector <number> protocol** (((all | ICMP | other | TCP | UDP) [dest-port (specific|not-specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (user|network|both)

**Syntax Description**

*number* Assigned number for attack-detector

*protocol* **TCP, UDP, ICMP, other**

*destination port* {TCP and UDP protocols only}: Defines whether the default attack detector applies to specific (port-based) or not specific (port-less) detections.

*attack-direction* *single-side-destination|single-side-both|dual-sided|all*

*side* **user, network, both**

*action* **report, block** (block is not currently supported.)

*open-flows-rate* Threshold for rate of open flows (new open flows per second).

*suspected-flows-rate* Threshold for for rate of suspected DDoS flows (new suspected flows per second)

---

*suspected-flows-ratio* Threshold for ratio of suspected flow rate to open flow rate.

---

---

#### Defaults

The default values for the default attack detector are:

- Action = Report
- Thresholds = Varies according to the attack type
- User notification = Disabled
- Sending an SNMP trap = Disabled

---

#### Command Modes

Linecard Interface Configuration

---

#### Usage Guidelines

If a specific attack detector is defined for a particular attack type, it will override the configured default attack detector.

The following arguments must always be specified:

- protocol
- attack-direction
- side

The following arguments are optional:

- action
- open-flows
- ddos-suspected-flows
- suspected-flows-ratio

Use the appropriate keyword to enable or disable user notification by default:

- **notify-user**: Enable user notification. (Use the [attack-filter user-notification ports](#) (on page 2-20) command to configure the port to be used for user notification.)
- **dont-notify-user**: Disable user notification.

Use the appropriate keyword to enable or disable sending an SNMP trap by default:

- **alarm**: Enable sending an SNMP trap.
- **no-alarm**: Disable sending an SNMP trap.

If the selected protocol is either TCP or UDP, specify whether the destination port is specific, not specific, or both. If the destination port or ports are specific, the specific destination ports are configured using the [attack-detector TCP-port-list/UDP-port-list](#) (on page 2-15) command.

Use the [attack-detector](#) (on page 2-11) command to enable a configured attack detector.

Use the [attack-detector default](#) (on page 2-9) command to configure a default attack detector.

Authorization: admin

The following examples illustrate the use of the **attack-detector <number>** command:

---

**Examples**
**EXAMPLE 1:**

The following example configures the attack detector number "2".

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# attack-detector 2 protocol UDP dest-port not-
specific attack-direction single-side-destination side both
action block open-flows-rate 500 suspected-flows-rate 500
suspected-flows-ratio 50 notify-user alarm
NME-APA(config if)#
```

**EXAMPLE 2:**

The following example deletes attack detector number "2".

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#no attack-detector 2
NME-APA(config if)#
```

**EXAMPLE 3:**

The following example disables user notification for attack detector number "2".

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-detector 2 protocol UDP dest-port not-
specific attack-direction single-side-destination side both dont-
notify-user
NME-APA(config if)#
```

---

**Related Commands**

[attack-detector](#) (on page 2-11)  
[attack-detector tcp-port-list/udp-port-list](#) (on page 2-15)  
[attack-filter user-notification ports](#) (on page 2-20)  
[attack-detector default](#) (on page 2-9)  
[show interface linecard attack-detector](#) (on page 2-139)

**attack-detector tcp-port-list|udp-port-list**

Defines the list of destination ports for specific port detections for TCP or UDP protocols.

**attack-detector** <number> (**tcp-port-list|udp-port-list**) (*all*|(<port1> [*<port2>* ...]))

**Syntax Description**

*number* number of the attack detector for which this list of specific ports is relevant

**Defaults**

This command has no default settings.

**Command Modes**

Linecard Interface Configuration

**Usage Guidelines**

TCP and UDP protocols may be configured for specified ports only (port-based). Use this command to configure the list of specified destination ports per protocol.

Up to 15 different TCP port numbers and 15 different UDP port numbers can be specified.

Configuring a TCP/UDP port list for a given attack detector affects only attack types that have the same protocol (TCP/UDP) and are port-based (i.e. detect a specific destination port). Settings for other attack types are not affected by the configured port list(s).

Specify either **TCP-port-list** or **UDP-port-list**.

Use the **all** keyword to include all ports in the list.

Authorization: admin

**Examples**

This example shows how to configure the destination port list for the TCP protocol for attack detector #10.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-detector 10 TCP-port-list 100 101 102
103
NME-APA(config if)#
```

**Related Commands**

[attack-detector <number>](#) (on page 2-12)

[attack-filter \(linecard Interface Configuration\)](#) (on page 2-16)

## attack-filter (Linecard Interface Configuration)

Enables specific attack detection for a specified protocol and attack direction.

Use the **no** form of the command to disable attack detection.

**attack-filter** [**protocol** (((TCP|UDP) [**dest-port** (specific|non-specific|both)]|ICMP|other)] [**attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all)]

**no attack-filter** [**protocol** (((TCP|UDP) [**dest-port** (specific|non-specific|both)]|ICMP|other)] [**attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all)]

### Syntax Description

*protocol* TCP, UDP, ICMP, or Other

*attack direction:* defines whether specific IP detection is enabled or disabled for single sided or dual sided attacks.

*destination port* (TCP and UDP protocols only): Defines whether specific IP detection is enabled or disabled for port-based (specific) or port-less (non-specific) detections.

### Defaults

By default, attack-filter is enabled.

Default *protocols* = all protocols (no protocol specified)

Default *attack direction* = all directions

Default *destination port* = oth port-based and port-less

### Command Modes

Linecard Interface Configuration

### Usage Guidelines

Specific attack filtering is configured in two steps:

- Enabling specific IP filtering for the particular attack type (using this command).
- Configuring an attack detector for the relevant attack type (using the [attack-detector <number>](#) (on page 2-12) command). Each attack detector specifies the thresholds that define an attack and the action to be taken when an attack is detected.

In addition, the user can manually override the configured attack detectors to either force or prevent attack filtering in a particular situation (using the [attack-filter \(Privileged Exec\)](#) (on page 2-18) command).

By default, specific-IP detection is enabled for all attack types. You can configure specific IP detection to be enabled or disabled for a specific, defined situation only, depending on the following options:

- For a selected protocol only.
- For TCP and UDP protocols, for only port-based or only port-less detections.
- For a selected attack direction, either for all protocols or for a selected protocol.

If the selected protocol is either TCP or UDP, specify whether the destination port is specific (port-based), not specific (port-less), or both. If the destination port or ports are specific, the specific destination ports are configured using the [attack-detector TCP-port-list/UDP-port-list](#) (on page 2-15) command.

Authorization: admin

---

## Examples

The following examples illustrate the use of this command.

### EXAMPLE 1

The following example shows how to enable specific, dual-sided attack detection for TCP protocol only.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-filter protocol TCP dest-port specific
attack-direction dual-sided
NME-APA(config if)#
```

### EXAMPLE 2

The following example shows how to enable single-sided attack detection for ICMP protocol only.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#attack-filter protocol ICMP attack-direction
single-side-source
NME-APA(config if)#
```

### EXAMPLE 3

The following example disables attack detection for all non TCP, UDP, or ICMP protocols.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#no attack-filter protocol other attack-
direction all
NME-APA(config if)#
```

---

## Related Commands

[attack-detector tcp-port-list/udp-port-list](#) (on page 2-15)

[attack-detector <number>](#) (on page 2-12)

[show interface linecard attack-filter](#) (on page 2-144)

## attack-filter (Privileged Exec)

The **attack-filter** command prevents attack filtering for a specified IP address/protocol. If filtering is already in process, it will be stopped.

When attack filtering has been stopped, it remains stopped until explicitly restored by another CLI command (either specific or general). Use the **no** form of this command to restore attack filtering.

The **force-filter** keyword forces attack filtering for a specified IP address/protocol. When attack filtering has been forced, it continues until explicitly stopped by another CLI command (either specific or general). Use the **no** form of this command to stop attack filtering.

**attack-filter** *slot-number* **ip** *ip-address* **protocol** *protocol* **attack-direction** *attack-direction* **side** *side* [**dont-filter**]

**attack-filter** *slot-number* **ip** *ip-address* **action** *action* **protocol** *protocol* **attack-direction** *attack-direction* **side** *side* [**force-filter**]

**no attack-filter** *slot-number* [**dont-filter**] [**all**]

**no attack-filter** *slot-number* [**force-filter**] [**all**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*ip-address* IP address from which traffic will not be filtered.

*action* *report*, *block* (block is not currently supported.)

*protocol* *TCP*, *UDP*, *IMCP*, *other*

*attack-direction* *attack-source*, *attack-destination*, *both*

*side* *user*, *network*, *both*

---

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC

### Usage Guidelines

After configuring the attack detectors, the NME-APA module automatically detects attacks and handles them according to the configuration. However, there are scenarios in which a manual intervention is desired, either for debug purposes, or because it is not trivial to reconfigure the NME-APA attack-detectors properly.

The user can use the CLI attack filtering commands to do the following:

- Prevent/stop filtering of an attack related to a specified IP address
- Force filtering of an attack related to a specified IP address

Attack filtering can be prevented for a specified IP address/protocol by executing a **dont-filter** CLI command. If filtering is already in process, it will be stopped. When attack filtering has been stopped, it remains stopped until explicitly restored by another CLI command (either **force-filter** or **no dont-filter**).

Attack filtering can be forced for a specified IP address/protocol. If filtering is already in process, it will be stopped. Forced attack filtering will continue until undone by an explicit CLI command (either **no force-filter** or **dont-filter**).

Use the all keyword to restore or stop all filtering.

Authorization: admin

---

## Examples

The following are examples of the **attack-filter** command:

### EXAMPLE 1:

The following example prevents attack filtering for the specified conditions.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#  
NME-APA#attack-filter 0 ip 10.10.10.10 protocol TCP attack-  
direction attack-source side both dont-filter  
NME-APA#
```

### EXAMPLE 2:

The following example restores all attack filtering.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#no attack-filter 0 dont-filter all  
NME-APA#
```

### EXAMPLE 3:

The following example forces attack filtering.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#attack-filter 0 action block ip 10.10.10.10 protocol TCP  
attack-direction attack-source side both  
NME-APA#
```

### EXAMPLE 4:

The following example stops all forced attack filtering.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#no attack-filter 0 force-filter all  
NME-APA#
```

---

## Related Commands

[attack-filter \(LineCard Interface Configuration\)](#) (on page 2-16)

[show interface linecard attack-filter](#) (on page 2-144)

## attack-filter user-notification ports

Specifies a port as user notification port. TCP traffic from the user side to this port will never be blocked by the attack filter, leaving it always available for user notification.

Use the **[no]** form of this command to remove the port from the user notification port list.

**attack-filter user-notification ports** *port*

**no attack-filter user-notification ports** *port*

|                    |                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>port</i> Port number. One port can be specified as the user notification port.                                                                                                                                                                                                                                  |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                                                                              |
| Command Modes      | Linecard Interface Configuration                                                                                                                                                                                                                                                                                   |
| Usage Guidelines   | Use this command to configure the port to be used for user notification as configured using the <a href="#">attack-filter (Linecard Interface Configuration)</a> (on page 2-16) and <a href="#">attack-detector &lt;number&gt;</a> (on page 2-12) commands.<br>Authorization: admin                                |
| Examples           | The following example specifies port 100 as the user notification port.<br><pre> <b>NME-APA&gt;enable 10</b> <b>Password:&lt;cisco&gt;</b> <b>NME-APA#config</b> <b>NME-APA(config)#interface linecard 0</b> <b>NME-APA(config if)#attack-filter user-notification ports 100</b> <b>NME-APA(config if)#</b> </pre> |
| Related Commands   | <a href="#">attack-detector default</a> (on page 2-9)<br><a href="#">attack-detector &lt;number&gt;</a> (on page 2-12)<br><a href="#">show interface linecard attack-filter</a> (on page 2-144) ( <b>user-notification ports</b> option)                                                                           |

## bandwidth

Sets Ethernet shaping for the FastEthernet line interfaces.

**bandwidth** *bandwidth* **burst-size** *burstsize*

---

### Syntax Description

*bandwidth* Bandwidth measured in kbps.

*burstsize* Burst size in bytes.

---



---

### Defaults

bandwidth = 100000K (100 Mbps)

burst-size = 5000 (5K bytes)

---

### Command Modes

FastEthernet Interface Configuration

---

### Usage Guidelines

This command is valid for a specified FastEthernet line interface only. It must be executed explicitly for each interface.

Use the [interface fastethernet](#) (on page 2-66) command to access the configuration mode for the desired interface.

Authorization: admin

---

### Examples

This example sets bandwidth and burst size for a Fast Ethernet line interface (0/1).

```
NME-APAconfig
NME-APA(config)#interface FastEthernet 0/1
NME-APA(config-if)#bandwidth 100000 burstsize 5000
NME-APA(config-if)#
```

---

### Related Commands

[interface fastethernet](#) (on page 2-66)

[queue](#) (on page 2-108)

## calendar set

Sets the system calendar. The calendar is a system clock that continues functioning even when the system shuts down.

**calendar set** *hh:mm:ss day month year*

| Syntax Description |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <i>hh:mm:ss</i>    | Current local time in hours in 24-hour format, minutes and seconds (HH:MM:SS). |
| <i>day</i>         | Current day (date) in the month.                                               |
| <i>month</i>       | Current month (by three-letter abbreviated name).                              |
| <i>year</i>        | Current year using a 4-digit number.                                           |

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

**Command Modes** Privileged EXEC

**Usage Guidelines** Always coordinate between the calendar and clock by using the `clock read-calendar` command after setting the calendar.

Authorization: admin

**Examples** The following example sets the calendar to 20 minutes past 10 AM, January 13, 2006, synchronizes the real-time clock to the calendar time, and displays the result.

```
NME-APA>enable 10
NME-APA#calendar set 10:20:00 13 jan 2006
NME-APA#clock read-calendar
NME-APA#show calendar
10:20:03 UTC THU January 13 2006
NME-APA#show clock
10:20:05 UTC THU January 13 2006
NME-APA#
```

**Related Commands**

- [clock read-calendar](#) (on page 2-33)
- [clock set](#) (on page 2-34)
- [clock update-calendar](#) (on page 2-40)
- [clock timezone](#) (on page 2-39)
- [clock summertime](#) (on page 2-35)
- [show calendar](#) (on page 2-129)
- [show clock](#) (on page 2-130)

**cd**

Changes the path of the current working directory.

**cd** *new-path*

**Syntax Description**

*new-path* The path name of the new directory. This can be either a full path or a relative path.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

The new path should already have been created in the local flash file system.

Authorization: admin

**Examples**

The following example shows the current directory (root directory) and then changes the directory to the log directory located under the root directory.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#pwd
tffs0
NME-APA#cd log
NME-APA#pwd
tffs0:log
NME-APA#
```

**Related Commands**

[pwd](#) (on page 2-107)

[mkdir](#) (on page 2-95)

## clear arp-cache

Deletes all dynamic entries from the ARP cache.

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses to physical addresses. Dynamic entries are automatically added to and deleted from the cache during normal use. Entries that are not reused age and expire within a short period of time. Entries that are reused have a longer cache life.

### clear arp-cache

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

Authorization: admin

---

#### Examples

The following example clears the ARP cache.

```
NME-APA>enable 10
NME-APA>password:<cisco>
NME-APA#clear arp-cache
NME-APA#
```

---

#### Related Commands

## clear interface linecard

Clears the linecard Interface counters.

**clear interface linecard** *slot-number* **counters**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example clears the Line-Card 0 counters.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#clear interface linecard 0 counters  
NME-APA#
```

---

### Related Commands

[show interface linecard counters](#) (on page 2-146)

## clear interface linecard traffic-counter

Clears the specified traffic counter.

**clear interface linecard** *slot-number* **traffic-counter** *name* [**all**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.  
*name* Name of the traffic counter to be cleared.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Use the **all** keyword to clear all traffic counters.

Authorization: admin

---

### Examples

The following example clears the traffic counter name counter1.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#clear interface linecard 0 traffic-counter name counter1
```

```
NME-APA#
```

---

### Related Commands

[traffic-counter](#) (on page 2-241)

[show interface linecard traffic-counter](#) (on page 2-154)

## clear interface linecard user

Clears all anonymous users in the system.

**clear interface linecard** *slot-number* **user anonymous all**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example clears all anonymous users.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#clear interface linecard 0 user anonymous all  
NME-APA#
```

---

### Related Commands

[no user](#) (on page 2-99)

[no user anonymous-group](#) (on page 2-100)

[show interface linecard user anonymous](#) (on page 2-159)

## clear interface linecard user db counters

Clears the “total” and “maximum” users database counters.

**clear interface linecard *slot-number* user db counters**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example clears all anonymous users.

```
NME-APA>enable 10
NME-APA>password:<cisco>
NME-APA#clear interface linecard 0 user db counters
NME-APA#
```

---

### Related Commands

[show interface linecard user db counters](#) (on page 2-161)

## clear logger

Clears NME-APA module logger (user log files). This erases the information stored in the user log files.

When using the **counters** keyword, it clears the counters of the NME-APA module logger (user log files). The counters keep track of the number of info, warning, error and fatal messages.

When using the **nv-counters** keyword, it clears the non-volatile counters for the entire log or only the specified NME-APA module. These counters are not cleared during bootup, and must be cleared explicitly by using this command.

**clear logger** [**device** *user-file-log/line-attack-file-log*] [**counters|nv-counters**]

---

### Syntax Description

*device*      The device name to be cleared, either user-file-log or line-attack-file-log

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

The users log files have a size limit, with new entries overwriting the oldest entries. Therefore, there is no need to regularly clear the log files. Use this operation when you are certain that the information contained on the logs is irrelevant and might be confusing (For example, when re-installing the system at a new site, whose administrators should not be confused with old information).

Authorization: admin

---

### Examples

The following examples illustrate the use of the **clear logger** command:

#### EXAMPLE 1:

The following example clears the NME-APA module user file logs:

```
NME-APA>enable 10
Password:<cisco>
NME-APA#clear logger device User-File-Log
Are you sure?Y
NME-APA#
```

**EXAMPLE 2:**

The following example clears the NME-APA module user log file counters.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#clear logger device User-File-Log counters  
Are you sure?Y  
NME-APA#
```

**EXAMPLE 3:**

The following example clears the user log file non-volatile counters.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#clear logger device user-file-log nv-counters  
Are you sure?Y  
NME-APA#
```

---

Related Commands

[show logger device](#) (on page 2-177)

[show log](#) (on page 2-176)

## clear management-agent notifications counters

Clears the counters for the number of notifications sent to the management agent.

### **clear management-agent notifications counters**

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example clears the management agent notifications counters.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#clear management-agent notifications counters
```

```
NME-APA#
```

---

**Related Commands**

## clear rdr-formatter

Clears the RDR formatter counters.

### **clear rdr-formatter**

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example clears the RDR-formatter counters.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#clear rdr-formatter  
NME-APA#
```

---

**Related Commands**

[show rdr-formatter counters](#) (on page 2-183)

## clock read-calendar

Synchronizes clocks by setting the system clock from the calendar.

### clock read-calendar

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example updates the system clock from the calendar.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#clock read-calendar  
NME-APA#
```

---

**Related Commands**

[calendar set](#) (on page 2-22)  
[clock update-calendar](#) (on page 2-40)  
[show calendar](#) (on page 2-129)  
[show clock](#) (on page 2-130)

## clock set

Manually sets the system clock.

**clock set** *hh:mm:ss day month year*

| Syntax Description |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <i>hh:mm:ss</i>    | Current local time in hours in 24-hour format, minutes and seconds (HH:MM:SS). |
| <i>day</i>         | Current day (date) in the month.                                               |
| <i>month</i>       | Current month (by three-letter abbreviated name).                              |
| <i>year</i>        | Current year using a 4-digit number.                                           |

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

**Command Modes** Privileged EXEC

**Usage Guidelines** Always coordinate between the calendar and clock by using the **clock update-calendar** command after setting the clock.  
Authorization: admin

**Examples** The following example sets the clock to 20 minutes past 10 PM, January 13, 2006.

```

NME-APA>enable 10
Password:<cisco>
NME-APA#clock set 22:20:00 13 jan 2006
NME-APA#clock update-calendar
NME-APA#show clock
22:21:10 UTC THU January 13 2006
NME-APA#show calendar
22:21:18 UTC THU January 13 2006
NME-APA#

```

**Related Commands** [clock update-calendar](#) (on page 2-40)  
[show calendar](#) (on page 2-129)  
[show clock](#) (on page 2-130)

## clock summertime

Configures the NME-APA module to automatically switch to daylight savings time on a specified date, and also to switch back to standard time. In addition, the three-letter time zone code can be configured to vary with daylight savings time if required. (For instance, in the eastern United States, standard time is designated EST, and daylight savings time is designated EDT).

Use the **no** form of this command to cancel the daylight savings time transitions configuration.

### clock summertime

#### no clock summertime

The format of the command varies somewhat, depending on how the dates for the beginning and end of daylight savings time are determined for the particular location:

- recurring: If daylight savings time always begins and ends on the same day every year, (as in the United States):
  - Use the **clock summer-time recurring** command
  - The *year* parameter is not used
- not recurring: If the start and end of daylight savings time is different every year, (as in Israel):
  - Use the **clock summer-time** command
  - The *year* parameter must be specified

General guidelines for configuring daylight savings time transitions:

- Specify the three letter time zone code for daylight savings time.
- recurring: specify a day of the month (week#|first|last/day of the week/month).
- not recurring: specify a date (month/day of the month/year).
- Define two days:
  - Day1 = beginning of daylight savings time.
  - Day2 = end of daylight savings time.

In the Southern hemisphere, month2 must be before month1, as daylight savings time begins in the fall and ends in the spring.

- Specify the exact time that the transition should occur (24 hour clock).
  - Time of transition into daylight savings time: according to local standard time.
  - Time of transition out of daylight savings time: according to local daylight savings time.

For the **clock summer-time recurring** command, the default values are the United States transition rules:

- Daylight savings time begins: 2:00 (AM) on the first Sunday of April.
- Daylight savings time ends: 2:00 (AM) on the last Sunday of October.

| Syntax Description   |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>zone</i>          | The 3-letter code for the time zone for daylight savings.                                                                                                                                                                                                                                                                                                                                                                                |
| <i>week1/week2</i>   | The week of the month on which daylight savings begins ( <i>week1</i> ) and ends ( <i>week2</i> ). A day of the week, such as Monday, must also be specified. The week/day of the week is defined for a recurring configuration only.<br>Default: Not used                                                                                                                                                                               |
| <i>day1/day2</i>     | The day of the week on which daylight savings begins ( <i>day1</i> ) and ends ( <i>day2</i> ).<br>For recurrent configuration: day is a day of the week, such as Sunday. Use the keywords first/last to specify the occurrence of a day of the week in a specified month: For example: last Sunday March.<br>For non-recurrent configuration: day is a day in the month, such as 28.<br>Default: day1 = first Sunday, day2 = last Sunday |
| <i>month1/month2</i> | The month in which daylight savings begins ( <i>month1</i> ) and ends ( <i>ends2</i> ).<br>Default: month1 = April, month2 = October                                                                                                                                                                                                                                                                                                     |
| <i>year1/year2</i>   | The year in which daylight savings begins ( <i>month1</i> ) and ends ( <i>ends2</i> ). For non-recurring configuration only.<br>Default = not used                                                                                                                                                                                                                                                                                       |
| <i>time1/time2</i>   | The time of day (24-hour clock) at which daylight savings begins ( <i>time1</i> ) and ends ( <i>time2</i> ). Required for all configurations.<br>Default: time1/time2 = 2:00                                                                                                                                                                                                                                                             |
| <i>offset</i>        | The difference in minutes between standard time and daylight savings time.<br>Default = 60                                                                                                                                                                                                                                                                                                                                               |

---

**Defaults**

recurring, offset = 60 minutes

By default, the following recurrent time changes are configured:

- Daylight savings time begins: 2:00 (AM) on the second Sunday of March.
- Daylight savings time ends: 2:00 (AM) on the first Sunday of November.

---

**Command Modes**

Global Configuration

---

**Usage Guidelines**

Use the **recurring** keyword to enable user notification.

Use the **first/last** keywords to specify the occurrence of a day of the week in a specified month: For example: last Sunday March.

Use a specific date including the year for a not recurring configuration. For example: March 29, 2004.

Use week/day of the week/month (no year) for a recurring configuration:

- Use first/last occurrence of a day of the week in a specified month. For example: last, Sunday, March (the last Sunday in March).

- Use the day of the week in a specific week in a specified month. For example: 4,Sunday, March (the fourth Sunday in March). This would be different from the last Sunday of the month whenever there were five Sundays in the month.

Authorization: admin

## Examples

The following examples illustrate the use of the **clock summertime** command:

### EXAMPLE 1:

The following example shows how to configure recurring daylight savings time for a time zone designated "DST" as follows:

- Daylight savings time begins: 0:00 on the last Sunday of March.
- Daylight savings time ends: 23:59 on the Saturday of fourth week of November.
- Offset = 1 hour (default)

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#clock summer-time DST recurring last Sunday March  
00:00 4 Saturday November 23:59
```

```
NME-APA(config)#
```

### EXAMPLE 2:

The following example shows how to configure non-recurring daylight savings time for a time zone designated "DST" as follows:

- Daylight savings time begins: 0:00 on April 16, 2005.
- Daylight savings time ends: 23:59 October 23, 2005.
- Offset = 1 hour (default)

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#clock summer-time DST April 16 2005 00:00  
October 23 2005 23:59
```

```
NME-APA(config)#
```

### EXAMPLE 3:

The following example shows how to cancel the daylight savings configuration.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#no clock summer-time
```

```
NME-APA(config)#
```

## Related Commands

[clock set](#) (on page 2-34)

[calendar set](#) (on page 2-22)

*show calendar* (on page [2-129](#))

*show clock* (on page [2-130](#))

## clock timezone

Sets the time zone. Use the no version of this command to remove current time zone setting. The purpose of setting the time zone is that the system can correctly interpret time stamps data coming from systems located in other time zones.

**clock timezone** *zone hours [minutes]*

**no clock timezone**

---

### Syntax Description

|                |                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>zone</i>    | The name of the time zone to be displayed.                                                                                                                                                        |
| <i>hours</i>   | The hours offset from GMT (UTC). This must be an integer in the range -23 to 23.                                                                                                                  |
| <i>minutes</i> | The minutes offset from GMT (UTC). This must be an integer in the range of 0 to 59. Use this parameter to specify an additional offset in minutes when the offset is not measured in whole hours. |

---



---

### Defaults

GMT (hours = 0)

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example sets the time zone to Pacific Standard Time with an offset of 10 hours behind GMT.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#clock timezone PST -10
NME-APA(config)#
```

---

### Related Commands

[calendar set](#) (on page 2-22)  
[clock set](#) (on page 2-34)  
[show calendar](#) (on page 2-129)  
[show clock](#) (on page 2-130)

## clock update-calendar

Synchronizes clocks by setting the calendar from the system clock.

### clock update-calendar

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example updates the calendar according to the clock.

```
NME-APA>enable 10
NME-APA>password:<cisco>
NME-APA#clock update-calendar
NME-APA#
```

---

**Related Commands**

[clock set](#) (on page 2-34)  
[calendar set](#) (on page 2-22)  
[clock read-calendar](#) (on page 2-33)  
[show calendar](#) (on page 2-129)  
[show clock](#) (on page 2-130)

## configure

Enables the user to move from Privileged Exec Mode to Configuration Mode.

### **configure**

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

After the user enters the **configure** command, the system prompt changes from <host-name># to <host-name> (config)#, indicating that the system is in Global Configuration Mode. To leave Global Configuration Mode and return to the Privileged Exec Mode prompt, type **exit**.

Authorization: admin

---

**Examples**

The following example enters the Global Configuration Mode.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#configure  
NME-APA(config)#
```

---

**Related Commands**

[exit](#) (on page 2-57)

## copy

Copies any file from a source directory to a destination directory on the local flash file system.

**copy** *source-file destination-file*

---

### Syntax Description

*source-file* The name of the original file.

*destination-file* The name of the new destination file.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Both file names should be in 8.3 format, that is, there are a maximum of 8 characters before the period and three characters following it.

Authorization: admin

---

### Examples

The following example copies the local analysis.sli file located in the root directory to the applications directory.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#copy analysis.sli applications/analysis.sli
```

```
NME-APA#
```

---

### Related Commands

[copy ftp://](#) (on page 2-43)

[copy-passive](#) (on page 2-44)

## copy ftp://

Downloads a file from a remote station to the local flash file system, using FTP.

**copy ftp://username[:password]@server-address[:port]/path/source-file destination-file**

---

### Syntax Description

*username* The username known by the FTP server.

*password* The password of the given username.

*server-address* The dotted decimal IP address of the FTP server.

*port* Optional port number on the FTP server.

*source-file* The name of the source file located in the on the server.

*destination-file* The name of the file to be saved in the local flash file system. The file should be in 8.3 format, that is 8 digits, dot, then 3 digits.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Use the following syntax for remote upload/download using FTP:

*ftp://username[:password]@server-address[:port]/path/file*

You can configure keyword shortcuts for the **copy** command using the following commands:

- *ip ftp password* (on page 2-75) to configure a password shortcut.
- *ip ftp username* (on page 2-76) to configure a username shortcut.

Authorization: admin

---

### Examples

The following example downloads the ftp.sli file from the host 10.1.1.105 with user name “vk” and password “vk”.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#copy ftp://vk:vk@10.1.1.105/p:/applications/ftp.sli
```

```
NME-APA#
```

---

### Related Commands

*copy-passive* (on page 2-44)

*ip ftp password* (on page 2-75)

*ip ftp username* (on page 2-76)

## copy-passive

Uploads or downloads a file using passive FTP.

**copy-passive** *source-file* **ftp://username[:password]@server-address[:port]/path/destination-file** **[overwrite]**

### Syntax Description

*source-file* The name of the source file located in the local flash file system.

*username* The username known by the FTP server.

*password* The password of the given username.

*server-address* The dotted decimal IP address.

*port* Optional port number on the FTP server.

*destination-file* The name of the file to be created in the FTP server.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC

### Usage Guidelines

Use the following format for remote upload/download using FTP:

**ftp://username[:password]@serveraddress[:port]/path/file**

Use the **overwrite** keyword to permit the command to overwrite an existing file.

You can configure keyword shortcuts for the **copy** command using the following commands:

- *ip ftp password* (on page 2-75) to configure a password shortcut.
- *ip ftp username* (on page 2-76) to configure a username shortcut.

Authorization: admin

### Examples

The following example performs the same operation as the previous copy ftp example using passive FTP.

```
NME-APA>enable 10
NME-APA>Password:<cisco>
NME-APA#copy-passive appl/analysis.sli
NME-APA#ftp://myname:mypw@10.1.1.105/p:/applications/analysis.sli
NME-APA#
```

### Related Commands

*copy ftp://* (on page 2-43)

*ip ftp password* (on page 2-75)

*ip ftp username* (on page 2-76)

## copy running-config startup-config

Builds a configuration file with general configuration commands called `config.txt`, which is used in successive boots.

### copy running-config startup-config

---

#### Syntax Description

---

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

This command must be entered to save newly configured parameters, so that they will be effective after a reboot. You can view the running configuration before saving it using the **more running-config** command.

The old configuration file is automatically saved in the `tffs0:system/prevconf` directory.

Authorization: admin

---

#### Examples

The following example saves the current configuration for successive boots.

```
NME-APA>enable 10
NME-APA>password <cisco>
NME-APA#copy running-config startup-config
Backing-up configuration file...
Writing configuration file...
NME-APA#
```

---

#### Related Commands

[more](#) (on page 2-96)

[show running-config](#) (on page 2-192)

## copy source-file ftp://

Uploads a file to a remote station, using FTP.

**copy** *source-file* **ftp://***username[:password]*@*server-address[:port]*/*path/destination-file*

---

### Syntax Description

*source-file* The name of the source file located in the local flash file system.

*username* The username known by the FTP server.

*password* The password of the given username.

*server-address* The dotted decimal IP address.

*port* Optional port number on the FTP server.

*destination-file* The name of the file to be created in the FTP server.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Use the following format for remote upload/download using FTP:

**ftp://username[:password]@serveraddress[:port]/path/file**

You can configure keyword shortcuts for the **copy** command using the following commands:

- **IP ftp password** to configure a password shortcut.
- **IP ftp userName** to configure a username shortcut.

Authorization: admin

---

### Examples

The following example uploads the analysis.sli file located on the local flash file system to the host 10.1.1.105.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#copy /appl/analysis.sli
```

```
ftp://myname:mypw@10.1.1.105/p:/applications/analysis.sli
```

```
NME-APA#
```

---

### Related Commands

[copy ftp://](#) (on page 2-43)

## copy source-file startup-config

Copies the specified source file to the startup-config file.

Use this command to upload a backup configuration file created using the **copy startup-config destination-file** command.

This is useful in a cascaded solution for copying the configuration from one NME-APA module to the other.

### **copy source-file startup-config**

---

#### Syntax Description

---

*source-file* The name of the backup configuration file.

```
ftp://user:pass@host/drive:/dir/bckupcfg.txt
```

---

```
/tffs0
```

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

The source file name should be in 8.3 format, that is, there are a maximum of 8 characters before the period and three characters following it.

Authorization: admin

---

#### Examples

The following example shows how to upload a backup configuration file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#copy ftp://user:pass@host/drive:/dir/bakupcfg.txt
startup-config
NME-APA#
```

---

#### Related Commands

[copy startup-config destination-file](#) (on page 2-48)

## copy startup-config destination-file

Copies the startup-config file to the specified destination file.

Use this command to create a backup configuration file.

This is useful in a cascaded solution for copying the configuration from one NME-APA module to the other. The file created by this command can then be uploaded to the second NME-APA module using the **copy source-file startup-config** command.

**copy startup-config** *destination-file*

---

### Syntax Description

*destination-file* The name of the file to which the configuration is copied.

```
ftp://user:pass@host/drive:/dir/bckupcfg.txt
/tffs0
```

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

The destination file name should be in 8.3 format, that is, there are a maximum of 8 characters before the period and three characters following it.

Authorization: admin

---

### Examples

The following example shows how to create a backup configuration file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#copy startup-config
ftp://user:pass@host/drive:/dir/bckupcfg.txt
NME-APA#
```

---

### Related Commands

[copy source-file startup-config](#) (on page 2-47)

## default user template all

Removes all user-defined user templates from the system. The default template only remains.

### default user template all

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

LineCard Interface Configuration

---

#### Usage Guidelines

Authorization: admin

---

#### Examples

The following example removes all user-defined user templates.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface LineCard 0
NME-APA(config if)# default user template all
NME-APA(config if)#
```

---

#### Related Commands

[user template import csv-file](#) (on page 2-254)

[show interface LineCard user templates](#) (on page 2-168)

## delete

Deletes a file from the local flash file system.

Use the recursive switch to delete a complete directory and its contents. When used with the recursive switch, the filename argument specifies a directory rather than a file.

**delete** *file-name* [/recursive]

---

|                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| Syntax Description | <i>file-name</i> The name of the file or directory to be deleted. |
|--------------------|-------------------------------------------------------------------|

---

|          |                                       |
|----------|---------------------------------------|
| Defaults | This command has no default settings. |
|----------|---------------------------------------|

|               |                 |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

|                  |                      |
|------------------|----------------------|
| Usage Guidelines | Authorization: admin |
|------------------|----------------------|

|          |                                                            |
|----------|------------------------------------------------------------|
| Examples | The following examples illustrate how to use this command: |
|----------|------------------------------------------------------------|

**EXAMPLE 1:**

The following example deletes the oldlog.txt file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#delete oldlog.txt
NME-APA#
```

**EXAMPLE 2:**

The following example deletes the oldlogs directory.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#delete oldlogs /recursive
3 files and 1 directories will be deleted.
Are you sure? y
3 files and 1 directories have been deleted.
NME-APA#
```

|                  |                                                                             |
|------------------|-----------------------------------------------------------------------------|
| Related Commands | <a href="#">dir</a> (on page 2-51)<br><a href="#">rmdir</a> (on page 2-118) |
|------------------|-----------------------------------------------------------------------------|

**dir**

Displays the files in the current directory.

**dir** [**applications**] [**-r**]

**Syntax Description**

**applications** Filters the list of files to display only the application files in the current directory.

**-r** Includes all files in the subdirectories of the current directory as well as the files in the current directory.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Authorization: admin

**Examples**

The following example displays the files in the current directory (root).

```
NME-APA>enable 10
Password:<cisco>
NME-APA#dir
File list for /tffs0/
512  TUE JAN 01 00:00:00 1980  LOGDBG          DIR
512  TUE JAN 01 00:00:00 1980  LOG             DIR
7653 TUE JAN 01 00:00:00 1980  FTP.SLI
29   TUE JAN 01 00:00:00 1980  SCRIPT.TXT
512  TUE JAN 01 00:00:00 1980  SYSTEM          DIR
NME-APA#
```

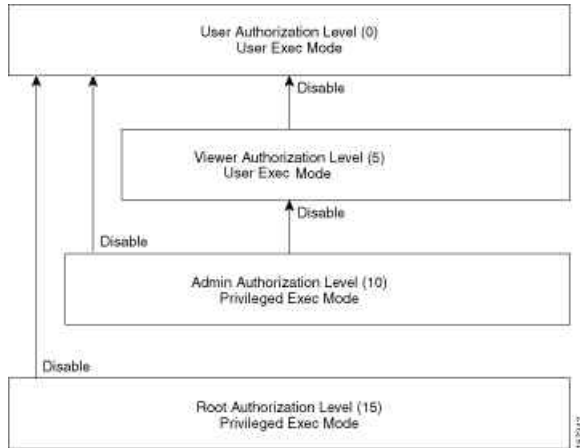
**Related Commands**

[pwd](#) (on page 2-107)

[cd](#) (on page 2-23)

## disable

Moves the user from a higher level of authorization to a lower user level, as illustrated in the following figure.



**disable** [*level*]

|                    |                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>level</i> User authorization level (0, 5, 10, 15) as specified in <a href="#">CLI Authorization Levels</a> (on page 1-5).                                                                                                                                      |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                             |
| Command Modes      | Privileged Exec and Viewer                                                                                                                                                                                                                                        |
| Usage Guidelines   | <p>Use this command with the level option to lower the user privilege level. If a level is not specified, it defaults to User mode.</p> <p>Note that you must <b>exit</b> to the Privileged Exec command mode to use this command.</p> <p>Authorization: user</p> |
| Examples           | <p>The following example shows how to change from root to admin mode:</p> <pre><b>NME-APA&gt;</b>enable 15 Password:&lt;cisco&gt; <b>NME-APA#&gt;</b>disable 10 <b>NME-APA#</b></pre>                                                                             |
| Related Commands   | <a href="#">enable</a> (on page 2-54)                                                                                                                                                                                                                             |

## do

Use the 'do' command to execute an EXEC mode command (such as a show command) or a privileged EXEC command (such as **show running-config**) without exiting to the relevant command mode.

### **do** *command*

---

**Syntax Description**

---

*command*    command to be executed.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

All configuration modes

---

**Usage Guidelines**

Use this command when in any configuration command mode (global configuration, linecard configuration, or any interface configuration) to execute a user exec or privileged exec command.

Enter the entire command with all parameters and keywords as you would if you were in the relevant command mode.

Authorization: admin

---

**Examples**

The following example assumes that the user has navigated to the interface configuration mode to perform some configuration tasks. The do command is used to avoid having to exit to the user exec mode.

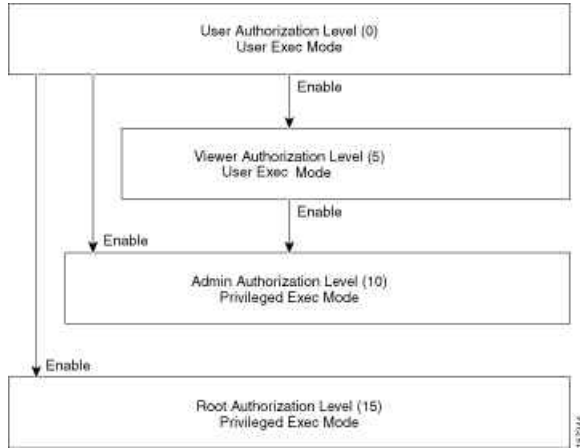
```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#do show system-uptime
NME-APA uptime is 20 hours, 43 minutes, 37 seconds
NME-APA(config if)#
```

---

**Related Commands**

## enable

Enables the user to access a higher authorization level, as illustrated in the following figure.



**enable** [*level*]

|                    |                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>level</i> User authorization level (0, 5, 10, 15) as specified in <a href="#">CLI Authorization Levels</a> (on page 1-5).                                                                                                                                                                         |
| Defaults           | level = admin                                                                                                                                                                                                                                                                                        |
| Command Modes      | User Exec                                                                                                                                                                                                                                                                                            |
| Usage Guidelines   | <p>If a level is not specified, the level defaults to admin authorization, level 10.</p> <p>Note that you cannot use the enable command from the Privileged Exec or any of the configuration command modes.</p> <p>Authorization: User</p>                                                           |
| Examples           | <p>The following example accesses the administrator authorization level. Note that the prompt changes from <i>NME-APA&gt;</i> to <i>NME-APA#</i>, indicating that the privilege is the administrator privilege level.</p> <pre><b>NME-APA&gt;</b>enable Password:&lt;cisco&gt; <b>NME-APA#</b></pre> |
| Related Commands   | <p><a href="#">disable</a> (on page 2-52)</p> <p><a href="#">enable password</a> (on page 2-55)</p>                                                                                                                                                                                                  |

## enable password

Configures a password for the specified authorization level, thus preventing unauthorized users from accessing the NME-APA module.

Use the **no** form of the command to disable the password for the specified authorization level.

**enable password** [**Level** *level*] [*encryption-type*] *password*

**no enable password** [**Level** *level*]

---

### Syntax Description

*level* User authorization level (0, 5, 10, 15) as specified in [CLI Authorization Levels](#) (on page 1-5). If no level is specified, the default is Admin (10).

*encryption-type* If you want to enter the encrypted version of the password, set the *encryption-type* to **5**, to specify the algorithm used to encrypt the password.

*password* A regular or encrypted password set for the access level. If you specify *encryption-type*, you must supply an encrypted password.

---



---

### Defaults

password = **cisco**

---

### Command Modes

Global Configuration

---

### Usage Guidelines

After the command is entered, any user executing the **enable** command must supply the specified password.

- Passwords must be at least 4 and no more than 100 characters long.
- Passwords can contain any printable characters.
- Passwords must begin with a letter.
- Passwords cannot contain spaces.
- Passwords are case-sensitive.

Authorization: admin

---

### Examples

The following example sets a level 10 password as a123\*man.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#enable password Level 10 a123*man
NME-APA(config)#
```

---

### Related Commands

[enable](#) (on page 2-54)

## erase startup-config-all

Removes all current configuration by removing all configuration files.

### erase startup-config-all

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

The following data is deleted by this command:

- General configuration files
- Application configuration files
- Static party DB files
- Management agent installed MBeans

After using this command, the NME-APA module should be reloaded immediately to ensure that it returns to the 'factory default' state.

You can use the [copy startup-config destination-file](#) (on page 2-48) command to create a backup of the current configuration before it is deleted.

Authorization: admin

---

#### Example

The following example shows how to erase the startup configuration.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#erase startup-config-all
```

---

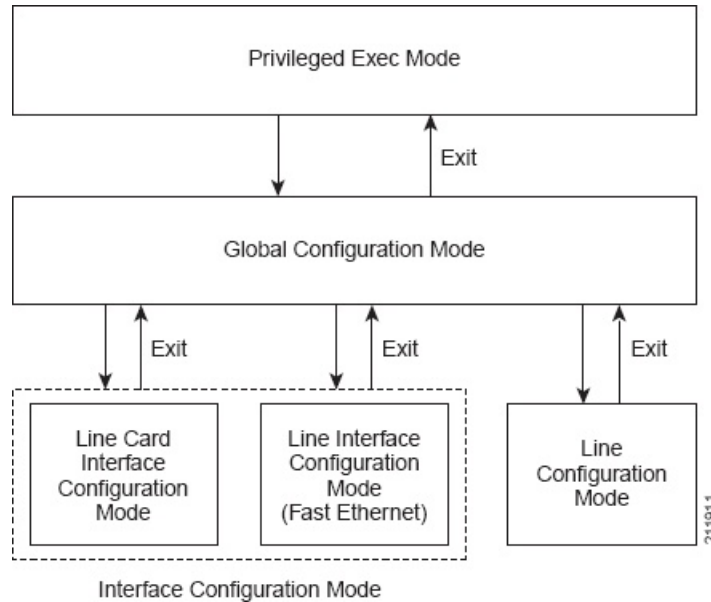
#### Related Commands

[reload](#) (on page 2-116)

[copy startup-config destination-file](#) (on page 2-48)

## exit

Exits from the current mode to the next "lower" mode, as illustrated in the following figure.



### exit

#### Syntax Description

This command has no arguments and keywords.

#### Defaults

This command has no default settings.

#### Command Modes

All

#### Usage Guidelines

Use this command each time you want to exit a mode. The system prompt changes to reflect the lower-level mode.

Authorization: admin

#### Examples

The following example exits from the Linecard Interface Configuration Mode to Global Configuration Mode and then to Privileged Exec and Viewer Modes.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#exit
NME-APA(config)#exit
NME-APA#
```

---

**Related Commands**

*configure* (on page 2-41)

*interface fastethernet* (on page 2-66)

*interface linecard* (on page 2-67)

*line vty* (on page 2-83)

## failure-recovery operation-mode

Specifies the operation mode to be applied after boot resulting from failure. When using the **default** switch, you do not have to specify the mode.

**failure-recovery operation-mode** *mode*

**default failure-recovery operation-mode**

|                    |                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>mode</i> <b>operational</b> or <b>non-operational</b> . Indicates whether the system will boot as operational or not following a failure.                                                                                                                              |
| Defaults           | mode = operational                                                                                                                                                                                                                                                        |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                      |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                                      |
| Examples           | <p>The following example sets the system to boot as operational after a failure</p> <pre><b>NME-APA&gt;enable 10</b> <b>Password:&lt;cisco&gt;</b> <b>NME-APA#config</b> <b>NME-APA(config)#failure-recovery operation-mode operational</b> <b>NME-APA(config)#</b></pre> |
| Related Commands   | <a href="#">show failure-recovery operation-mode</a> (on page 2-131)                                                                                                                                                                                                      |

## force failure-condition

Forces a virtual failure condition, and exits from the failure condition, when performing an application upgrade.

**force failure-condition**

**no force failure-condition**

---

### Syntax Description

This command has no arguments or keywords

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example forces a virtual failure condition.

```
NME-APA>enable 10
NME-APA>Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#force failure-condition
NME-APA(config if)#
```

---

### Related Commands

[pqf upgrade file](#) (on page 2-106)

## help

Displays information relating to all available CLI commands.

**help bindings|tree**

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Exec

---

**Usage Guidelines**

Use the *bindings* keyword to print a list of keyboard bindings (shortcut commands).

Use the *tree* keyword to display the entire tree of all available CLI commands.

Authorization: User

---

**Examples**

The following example shows the partial output of the help bindings command.

```
NME-APA>help bindings
```

```
Line Cursor Movements
```

```
-----
```

```
Ctrl-F /-> Moves cursor one character to the right.
```

```
Ctrl-B /<- Moves cursor one character to the left.
```

```
Esc-F      Moves cursor one word to the right.
```

```
Esc-B      Moves cursor one word to the left.
```

```
Ctrl-A      Moves cursor to the start of the line.
```

```
Ctrl-E      Moves cursor to the end of the line.
```

```
Esc F       Moves cursor forward one word.
```

```
Esc B       Moves cursor backward one word.
```

## Editing

-----

Ctrl-D                   Deletes the character where the cursor is located.

Esc-D                   Deletes from the cursor position to the end of the word.

Backspace               Deletes the character before the current location of the cursor.

Ctrl-H                   Deletes the character before the current location of the cursor.

Ctrl-K                   Deletes from the cursor position to the end of the line.

Ctrl-U                   Deletes all characters from the cursor to the beginning of the line.

Ctrl-X                   Deletes all characters from the cursor to the beginning of the line.

Ctrl-W                   Deletes the word to the left of the cursor.

Ctrl-Y                   Recall the last item deleted.

## Help and Operation Features

-----

?                       Argument help.

<Tab>                   Toggles between possible endings for the typed prefix.

<Esc><Tab>             Displays all the possible arguments backwards.

Ctrl-I                   <TAB>

**NME-APA>**

---

 Related Commands

## history

Enables the history feature, that is, a record of the last command lines that executed. Use the **no** form of this command to disable history.

**history**

**no history**

---

### Syntax Description

This command has no arguments or keywords.

---



---

### Defaults

History is enabled.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following examples illustrate how to use this command.

#### EXAMPLE 1

The following example enables the **history** feature.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#history
NME-APA#
```

#### EXAMPLE 2

The following example disables the **history** feature.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#no history
NME-APA#
```

---

### Related Commands

[history size](#) (on page 2-64)

## history size

Sets the number of command lines that the system records in the history.

**history size** *size*

**no history size**

---

|                    |                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------|
| Syntax Description | <i>size</i> The number of command lines stored in the history of commands for quick recall. |
|--------------------|---------------------------------------------------------------------------------------------|

---

|          |                 |
|----------|-----------------|
| Defaults | size = 10 lines |
|----------|-----------------|

|               |                 |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

|                  |                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | The size of the history buffer can be any number from 0-50. Use the [ <b>no</b> ] form of this command to restore the default size. |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|

Authorization: admin

|          |                                                                         |
|----------|-------------------------------------------------------------------------|
| Examples | The following example sets the history buffer size to 50 command lines. |
|----------|-------------------------------------------------------------------------|

```
NME-APA>enable 10
Password:<cisco>
NME-APA#history size 50
NME-APA#
```

|                  |                                        |
|------------------|----------------------------------------|
| Related Commands | <a href="#">history</a> (on page 2-63) |
|------------------|----------------------------------------|

## hostname

Modifies the name of the NME-APA module. The host name is part of the displayed prompt.

**hostname** *host-name*

---

### Syntax Description

---

*host-name* The new host name. Maximum length is 20 characters.

---

---

### Defaults

host-name = *NME-APA*

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example changes the host name to MyHost.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#>hostname MyHost
MyHost(config)#>
```

---

### Related Commands

[show hostname](#) (on page 2-132)

## interface fastethernet

Enters FastEthernet Interface Configuration mode to configure a specified Fast Ethernet line interface.

**interface fastethernet** *slot-number/interface-number*

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of **0**.

*interface-number* The FastEthernet interface number. Enter a value between **1** and **2** to configure one of the line ports for an NME-APA module.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

This command is used to configure the line ports.

To return to the Global Configuration Mode, type **exit**.

The system prompt changes to reflect the Fast Ethernet Interface Configuration mode.

Authorization: admin

---

### Examples

The following example enters into FastEthernet Configuration Interface Mode for line port #1.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface fastethernet 0/1
NME-APA(config if)#
```

[exit](#) (on page 2-57)

---

### Related Commands

[show interface fastethernet](#) (on page 2-134)

[interface fastethernet](#) (on page 2-66)

## interface linecard

Enters Linecard Interface Configuration Mode.

**interface linecard** *slot-number*

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

The system prompt is changed to reflect the Line Card Configuration mode. To return to the Global Configuration Mode, type **exit**.

Authorization: admin

---

### Examples

The following example enters LineCard Interface Configuration Mode.

```
NME-APA(config)#interface linecard 0
```

```
NME-APA(config if)#
```

---

### Related Commands

[exit](#) (on page 2-57)

## ip advertising

Enables IP advertising. If the destination and/or interval is not configured, the default values are assumed.

Use the **no** version of the command to disable IP advertising.

Use the **default** version of the command to restore IP advertising destination or interval to the default values.

**ip advertising** [**destination** *destination*] [**interval** *interval*]

**no ip advertising**

**default ip advertising** [**destination** | **interval**]

---

### Syntax Description

*destination* The IP address of the destination for the ping requests

*interval* The frequency of the ping requests in seconds

---



---

### Defaults

By default, IP advertising is disabled

destination = 127.0.0.1

interval = 300 seconds

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following examples illustrate the use of the **ip advertising** command:

**EXAMPLE 1:**

The following example enables IP advertising, specifying 10.1.1.1 as the destination and an interval of 240 seconds.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#ip advertising destination 10.1.1.1 interval 240
```

```
NME-APA(config)#
```

**EXAMPLE 2:**

The following example restores the IP advertising destination to the default value.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#default ip advertising destination
```

```
NME-APA(config)#
```

---

**Related Commands**

[show ip advertising](#) (on page 2-170)

## ip domain-lookup

Enables or disables the domain name lookups.

Use the **no** form of the command to disable the domain name lookup.

**ip domain-lookup**

**no ip domain-lookup**

### Syntax Description

This command has no arguments or keywords.

### Defaults

By default, domain name lookup is enabled.

### Command Modes

Global Configuration

### Usage Guidelines

Authorization: admin

### Examples

The following examples illustrate how to use this command.

#### EXAMPLE 1:

The following example enables the domain lookup.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#ip domain-lookup
NME-APA(config)#
```

#### EXAMPLE 2:

The following example disables the domain lookup.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#no ip domain-lookup
NME-APA(config)#
```

### Related Commands

[ip domain-name](#) (on page 2-71)

[ip name-server](#) (on page 2-78)

[show hosts](#) (on page 2-133)

## ip domain-name

Defines a default domain name. Use the **no** parameter of this command to remove the current default domain name. When using the **no** parameter, you do not have to specify the domain name.

**ip domain-name** *domain-name*

**no ip domain-name**

---

### Syntax Description

*domain-name* The default domain name used to complete host names that do not specify a domain. Do not include the initial period that separates an unqualified name from the domain name.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following examples illustrate the use of the **ip domain-name** command:

#### EXAMPLE 1:

The following example configures the domain name.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#ip domain-name Cisco.com
NME-APA(config)#
```

#### EXAMPLE 2:

The following example removes the configured domain name.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#no ip domain-name
NME-APA(config)#
```

---

### Related Commands

[ip domain-lookup](#) (on page 2-70)

[ip name-server](#) (on page 2-78)

[show hosts](#) (on page 2-133)

## ip filter fragment

Use this command to enable the filtering out of IP fragments.

**ip filter fragment enable**

**ip filter fragment disable**

---

### Syntax Description

This command has no arguments or keywords.

---



---

### Defaults

By default, IP fragment filtering is disabled.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Management security is defined as the capability of the NME-APA module to cope with malicious management conditions that might lead to global service failure.

There are two parallel security mechanisms:

- Automatic security mechanism — monitors the TCP/IP stack rate at 200 msec intervals and throttles the rate from the device if necessary.
- User-configurable security mechanism — accomplished via two IP filters at user-configurable intervals:
  - IP fragment filter: Drops all IP fragment packets
  - IP filter monitor: Measures the rate of accepted and dropped packets for both permitted and not-permitted IP addresses.

This command enables the IP fragment filter.

Use the [ip filter monitor](#) (on page 2-73) command to configure the IP filter monitor.

Use the **enable** keyword to enable IP fragment filtering.

Use the **disable** keyword to disable IP fragment filtering.

Authorization: admin

---

### Examples

The following example shows how to enable IP fragment filtering.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#ip filter fragment enable
NME-APA(config)#
```

---

### Related Commands

[ip filter monitor](#) (on page 2-73)

[show ip filter](#) (on page 2-171)

## ip filter monitor

Configures the limits for permitted and not-permitted IP address transmission rates.

**ip filter monitor** {**ip\_permitted** | **ip\_not\_permitted**} **low\_rate** *low\_rate* **high\_rate** *high\_rate*  
**burst** *burst size*

### Syntax Description

|                   |                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>low_rate</i>   | lower threshold; the rate in Mbps that indicates the attack is no longer present                                                                       |
| <i>high_rate</i>  | upper threshold; the rate in Mbps that indicates the presence of an attack                                                                             |
| <i>burst size</i> | duration of the interval in seconds that the high and low rates must be detected in order for the threshold rate to be considered to have been reached |

### Defaults

low rate = 20 Mbps

high rate = 20 Mbps

burst size = 10 seconds

### Command Modes

Global Configuration

### Usage Guidelines

Management security is defined as the capability of the NME-APA module to cope with malicious management conditions that might lead to global service failure.

There are two parallel security mechanisms:

- Automatic security mechanism — monitors the TCP/IP stack rate at 200 msec intervals and throttles the rate from the device if necessary.
- User-configurable security mechanism — accomplished via two IP filters at user-configurable intervals:
  - IP fragment filter: Drops all IP fragment packets
  - IP filter monitor: Measures the rate of accepted and dropped packets for both permitted and not-permitted IP addresses.

This command configures the IP filter monitor.

Use the [ip filter fragment](#) (on page 2-72) command to enable the IP fragment filter.

Use the **ip permitted** keyword to apply configured limits to permitted IP addresses.

Use the **ip not-permitted** keyword to apply configured limits to not-permitted IP addresses.

If neither keyword is used, it is assumed that the configured limits apply to both permitted and not-permitted IP addresses.

Authorization: admin

---

**Examples**

The following example shows how to configure the rates for permitted IP addresses.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)# ip filter monitor ip permitted low_rate 25
high_rate 30 burst 15
NME-APA(config)#
```

---

**Related Commands**

[ip filter fragment](#) (on page 2-72)

[show ip filter](#) (on page 2-171)

## ip ftp password

Specifies the password to be used for FTP connections for the current session. The system will use this password if no password is given in the copy FTP command.

**ip ftp password** *password*

---

### Syntax Description

*password* The password for FTP connections.

---

Default password is **admin**

---

### Defaults

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example sets the password to be used in the FTP connection to mypw.

```
NME-APA>enable 10
NME-APA>password:<cisco>
NME-APA#ip ftp password mypw
NME-APA#
```

---

### Related Commands

[copy ftp://](#) (on page 2-43)

[copy-passive](#) (on page 2-44)

[ip ftp username](#) (on page 2-76)

## ip ftp username

Configures the username for FTP connections for the current session. This username will be used if no username is given in the copy FTP command.

**ip ftp username** *user-name*

### Syntax Description

*user-name* The username for FTP connections.

### Defaults

Default username is **anonymous**

### Command Modes

Privileged EXEC

### Usage Guidelines

Authorization: admin

### Examples

The following example sets *myname* as the username for FTP connections.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#ip ftp username myname
NME-APA#
```

### Related Commands

[copy ftp://](#) (on page 2-43)  
[copy-passive](#) (on page 2-44)  
[ip ftp password](#) (on page 2-75)

## ip host

Adds a host name and address to the host table.

Use the **no** form of the command to remove a host name and address from the host table.

**ip host** *hostname ip-address*

**no ip host** *hostname [ip-address]*

---

### Syntax Description

*hostname* The host name to be added or removed.

*ip-address* The host IP address in x.x.x.x format.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example adds a host to the host table.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#ip host PC85 10.1.1.1
NME-APA(config)#
```

---

### Related Commands

[show hosts](#) (on page 2-133)

## ip name-server

Specifies the address of 1–3 servers to use for name and address resolution. The system maintains a list of up to 3 name servers. If the current list is not empty, this command adds the specified servers to the list. The no option of this command removes specified servers from the current list.

**ip name-server** *server-address1* [*server-address2*] [*server-address3*]

**no ip name-server**

### Syntax Description

*server-address1* The IP address of the name server.

*server-address2* The IP address of an additional name server.

*server-address3* The IP address of an additional name server.

### Defaults

This command has no default settings.

### Command Modes

Global Configuration

### Usage Guidelines

Authorization: admin

### Examples

The following example adds the DNS 10.1.1.1 and 10.1.1.2 to the configured servers list.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#ip name-server 10.1.1.1 10.1.1.2
NME-APA(config)#
```

### Related Commands

[ip domain-lookup](#) (on page 2-70)

[show hosts](#) (on page 2-133)

## ip radius-client retry limit

Configures the parameters for retransmitting unacknowledged messages.

**ip radius-client retry limit** *times* [**timeout** *timeout*]

### Syntax Description

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| <i>times</i>   | The maximum number of times the RADIUS client can try unsuccessfully to send a message. |
| <i>timeout</i> | Timeout interval for retransmitting a message, in seconds                               |

### Defaults

*times* = 3  
*timeout* = 5 second

### Command Modes

Global Configuration

### Usage Guidelines

Due to the unreliable nature of UDP, the RADIUS client retransmits requests to the SCMP peer device if they were not acknowledged within the configured number of seconds. Messages that were not acknowledged can be retransmitted up to the configured maximum number of retries.

The optional *timeout* parameter limits the time interval for retransmitting a message.

Authorization: admin

### Examples

The following example illustrates how to configure the retransmission parameters.

```
NME-APA>enable 10
NME-APA>Password:<cisco>
NME-APA#config
NME-APA(config)# ip radius-client retry limit 5 timeout 5
NME-APA(config)#
```

[show ip radius-client](#) (on page 2-173)

### Related Commands

## ip rpc-adapter

Enables the RPC adapter. Use the **no** option of this command to disable the RPC adapter.

**ip rpc-adapter**

**no ip rpc-adapter**

|                    |                                           |
|--------------------|-------------------------------------------|
| Syntax Description | This command has no arguments or keywords |
|--------------------|-------------------------------------------|

|          |                                       |
|----------|---------------------------------------|
| Defaults | This command has no default settings. |
|----------|---------------------------------------|

|               |                      |
|---------------|----------------------|
| Command Modes | Global Configuration |
|---------------|----------------------|

|                  |                      |
|------------------|----------------------|
| Usage Guidelines | Authorization: admin |
|------------------|----------------------|

|          |                                                                                 |
|----------|---------------------------------------------------------------------------------|
| Examples | The following examples illustrate the use of the <b>ip rpc-adapter</b> command: |
|----------|---------------------------------------------------------------------------------|

### EXAMPLE 1:

The following example enables the RPC adapter.

```

NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#ip rpc-adapter
NME-APA(config)#

```

### EXAMPLE 2:

The following example disables the RPC adapter.

```

NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#no ip rpc-adapter
NME-APA(config)#

```

|                  |                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Related Commands | <p><i>ip rpc-adapter port</i> (on page 2-81)</p> <p><i>show ip rpc-adapter</i> (on page 2-174)</p> <p><i>ip rpc-adapter security-level</i> (on page 2-82)</p> |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|

## ip rpc-adapter port

Defines the RPC adapter port. Use the **default** option to reset the RPC adapter port assignment to the default port of 14374.

**ip rpc-adapter port** *port-number*

**default ip rpc-adapter port**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>port-number</i> The number of the port assigned to the RPC adapter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Defaults           | port number = 14374                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Examples           | <p>The following examples illustrate the use of the <b>ip rpc-adapter port</b> command:</p> <p><b>EXAMPLE 1:</b></p> <p>The following example shows how to configure the RPC interface, specifying 1444 as the RPC adapter port.</p> <pre>NME-APA&gt;enable 10 Password:&lt;cisco&gt; NME-APA#config NME-APA(config)#ip rpc-adapter NME-APA(config)#ip rpc-adapter port 1444</pre> <p><b>EXAMPLE 2:</b></p> <p>The following example shows how reset the RPC adapter port.</p> <pre>NME-APA&gt;enable 10 Password:&lt;cisco&gt; NME-APA#config NME-APA(config)#default ip rpc-adapter port</pre> |
| Related Commands   | <p><a href="#">ip rpc-adapter</a> (on page 2-80)</p> <p><a href="#">show ip rpc-adapter</a> (on page 2-174)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## ip rpc-adaptor security-level

Sets the PRPC server security level.

**ip rpc-adaptor security-level {full|semi|none}**

---

**Syntax Description**

---

full|semi|none

---

---

**Defaults**

default = semi

---

**Command Modes**

Global Configuration

---

**Usage Guidelines**

Specify the desired PRPC server security level:

- full: all PRPC connections require authentication
- semi: PRPC connections that supply a user-name and password during connection establishment are authenticated. Connections that do not supply a user-name and password are accepted with no authentication
- none: no authentication is performed

Authorization: admin

---

**Examples**

The following example illustrates how to set the PRPC server security level.

```

NME-APA>enable 10
Password:<cisco>
NME-APA#configure
NME-APA(config)#ip rpc-adaptor security-level full
NME-APA>

```

---

**Related Commands**

[ip rpc-adapter](#) (on page 2-80)

[show ip rpc-adapter](#) (on page 2-174)

## line vty

Enters Line Configuration Mode for Telnet lines, configuring all Telnet lines.

**line vty** *start-number* [*end-number*]

---

### Syntax Description

*start-number* A number in the range 0-4. The actual number supplied does not matter. All telnet lines will be configured by this command.

*end-number* A number in the range 0-4. The actual number supplied does not matter. All telnet lines will be configured by this command.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

The system prompt changes to reflect the Line Configuration mode. To return to Global Configuration Mode, type *exit* (on page 2-57).

Authorization: admin

---

### Examples

The following example enters the Line Configuration Mode for all lines.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#config  
NME-APA(config)#line vty 0  
NME-APA(config-line)#
```

---

### Related Commands

*show line vty* (on page 2-175)

*exit* (on page 2-57)

## link mode

Configures the link mode. The link mode allows the user to enforce the specified behavior on the link. This may be useful during installation and for debugging the network.

**link mode** *link mode*

---

### Syntax Description

|             |                                                        |
|-------------|--------------------------------------------------------|
| <i>link</i> | FE: <b>port1</b><br><b>port2</b><br><b>port1-port2</b> |
| <i>mode</i> | <b>Forwarding</b><br><b>Bypass</b>                     |

---



---

### Defaults

---

### Command Modes

Linecard Interface Configuration

Use the **port1-port2** keyword to configure the link mode for all links.

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following examples illustrate the use of the link mode command:

**EXAMPLE 1:**

The following example configures "bypass" as the link mode on the first link for the NME-APA module.

```
NME-APA Module>enable 10
Password:<cisco>
NME-APA Module#config
NME-APA Module(config)#interface linecard 0
NME-APA Module(config if)#link mode port1 bypass
NME-APA Module(config if)#
```

**EXAMPLE 2:**

The following example configures "forwarding" as the link mode for the NME-APA module.

```
NME-APA Module>enable 10
Password:<cisco>
NME-APA Module#config
NME-APA Module(config)#interface linecard 0
NME-APA Module(config if)#link mode forwarding
NME-APA Module(config if)#
```

---

**Related Commands**

[show interface linecard link mode](#) (on page 2-149)

## logger add-user-message

Adds a message string to the user log files.

**logger add-user-message** *message-text*

---

### Syntax Description

---

*message-text* The message string you wish to add.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example adds "testing 123" as the message to the user log files:

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#logger add-user-message testing 123  
NME-APA#
```

---

### Related Commands

## logger device

Disables or enables the logger device. Available logger devices are:

- Line-Attack-File-Log
- Statistics-Archive-File-Log
- User-File-Log

**logger device** {**line-attack-file-log** | **statistics-file-log** | **user-file-log**} *status*

---

### Syntax Description

*status*      **enabled** or **disabled**, indicating whether to turn on or off logging.

---



---

### Defaults

By default, the log devices are enabled.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example disables the User-File-Log device.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#logger device user-file-log disabled
NME-APA(config)#
```

---

### Related Commands

[logger device user-file-log max-file-size](#) (on page 2-88)

[show logger device](#) (on page 2-177)

[logger get user-log file-name](#) (on page 2-90)

[clear logger](#) (on page 2-29)

## logger device user-file-log max-file-size

Sets the maximum log file size.

### logger device user-file-log max-file-size

|                    |                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>size</i> The maximum size for the user log (in bytes).                                                                                                                                                                                                                                        |
| Defaults           | 1,000,000 bytes                                                                                                                                                                                                                                                                                  |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                                             |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                                                             |
| Examples           | <p>The following example configures the maximum size of the User-File-Log device to 65000 bytes.</p> <pre> <b>NME-APA&gt;</b>enable 10 Password:&lt;<i>cisco</i>&gt; <b>NME-APA#</b>config <b>NME-APA(config)#</b>logger device user-file-log max-file-size 65000 <b>NME-APA(config)#</b> </pre> |
| Related Commands   | <p><a href="#">logger device</a> (on page 2-87)</p> <p><a href="#">show logger device</a> (on page 2-177)</p>                                                                                                                                                                                    |

## logger get support-file

Generates a log file for technical support. Note that this operation may take some time.

**logger get support-file** *filename*

---

### Syntax Description

---

*filename* Name of the generated log file.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example generates a log file named *tech\_sup* for technical support.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#logger get support-file tech_sup  
NME-APA#
```

---

### Related Commands

[logger get user-log file-name](#) (on page 2-90)

## logger get user-log file-name

Outputs the current user log to a target file. The output file name can be a local path, full path, or full ftp path file name.

**logger get user-log file-name** *target-file*

---

|                    |                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------|
| Syntax Description | <i>target-file</i> The log file name where the system will write the log file information. |
|--------------------|--------------------------------------------------------------------------------------------|

---

|          |                                       |
|----------|---------------------------------------|
| Defaults | This command has no default settings. |
|----------|---------------------------------------|

---

|               |                 |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

---

|                  |                      |
|------------------|----------------------|
| Usage Guidelines | Authorization: admin |
|------------------|----------------------|

---

|          |                                                                                                                                                                                                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Examples | <p>The following example retrieves the current user log files.</p> <pre><b>NME-APA&gt;</b>enable 10 Password:&lt;<i>cisco</i>&gt; <b>NME-APA#</b>logger get user-log file-name <i>ftp://myname:mypw@10.1.1.205/d:/log.txt</i> <b>NME-APA#</b></pre> |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                  |                                                        |
|------------------|--------------------------------------------------------|
| Related Commands | <a href="#">logger get support-file</a> (on page 2-89) |
|------------------|--------------------------------------------------------|

## logout

Logs out of the Command-Line Interface of the NME-APA module.

### **logout**

---

**Syntax Description**

---

This command has no arguments or keywords

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Exec

---

**Usage Guidelines**

The system prompts for confirmation of the **logout** command with 'N'. Type 'Y' to confirm the logout.

Authorization: User

---

**Examples**

The following example shows how the user logs out (and confirms the logout).

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#config  
NME-APA(config)#exit  
NME-APA>logout  
Are you sure? Y
```

---

**Related Commands**

## management-agent sce-api logging

Enables the SCE user API trouble-shooting logging, which is written to the user-log.

Use the **no** form of this command to disable SCE user API trouble-shooting logging.

**management-agent sce-api logging**

**no management-agent sce-api logging**

---

### Syntax Description

This command has no arguments or keywords

---



---

### Defaults

By default, the SCE user API trouble-shooting logging is disabled.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example enables SCE user API trouble-shooting logging.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)# management-agent sce-api logging
NME-APA(config)#
```

---

### Related Commands

## management-agent sce-api timeout

Defines the timeout interval for disconnection of an SCE user API client, after which the resources allocated for this client would be released.

**management-agent sce-api timeout** *timeout-interval*

---

### Syntax Description

*timeout-interval* default time in seconds that the client waits before timing out.

---



---

### Defaults

Default = 300 seconds

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

This example shows how to configure a timeout interval of 10 seconds.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)# management-agent sce-api timeout 10
```

---

### Related Commands

## management-agent system

Specifies a new package file to install for the management agent. The NME-APA module extracts the actual image file(s) from the specified package file only during the **copy running-config startup-config** command.

When using the **no** version of this command, you do not have to specify the package-file-name.

**management-agent system** *package-file-name*

**no management-agent system**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>package-file-name</i> The name of a package file that contains the new management agent software. The filename should end with the .pkg extension.                                                                                                                                                                                                                                                                                                                             |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Usage Guidelines   | <p>Use this command to upgrade the NME-APA module management agent. The package file is verified for the system and checked that it is not corrupted. The actual upgrade takes place only after executing the <a href="#">copy running-config startup-config</a> (on page 2-45) command and rebooting the NME-APA module.</p> <p>Authorization: admin</p>                                                                                                                         |
| Examples           | <p>The following example upgrades the system with the <i>mng45.pkg</i> package.</p> <pre><b>NME-APA&gt;</b>enable 10 Password:&lt;<i>cisco</i>&gt; <b>NME-APA#</b>config <b>NME-APA(config)#management-agent system</b> <i>mng45.pkg</i> Verifying package file... Package file verified OK. <b>NME-APA(config)#do copy running-config startup-config</b> Backing -up configuration file... Writing configuration file... Extracting new management agent...  Extracted OK.</pre> |
| Related Commands   | <a href="#">copy running-config startup-config</a> (on page 2-45)                                                                                                                                                                                                                                                                                                                                                                                                                 |

## mkdir

Creates a new directory.

**mkdir** *directory-name*

---

### Syntax Description

---

*directory-name* The name of the directory to be created.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example creates a new directory named mydir.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#mkdir mydir  
NME-APA#
```

---

### Related Commands

[dir](#) (on page 2-51)

**more**

Displays the contents of a file.

**more** {*file-name* | **running-config** [**all-data**] | **startup-config**}

**Syntax Description**

*file-name* The name of the file to be displayed.

**all data** Displays defaults as well as non-default settings (running-config option only)

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

The **running-config** option displays the running configuration file. You can use the **all data** switch with this option to see sample usage for many CLI configuration commands.

The **startup-config** option displays the startup configuration file.

Authorization: admin

**Examples**

The following sample output displays the contents of the running configuration file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#more running-config
#This is a general configuration file (running-config).
#Created on 16:48:11 UTC WED June 13 2001

cli-type 1
#version 1

service logger

no service password-encryption
enable password level 10 0 "cisco"
enable password level 15 0 "cisco"
service RDR-formatter
no RDR-formatter destination all
RDR-formatter history-size 0
clock timezone UTC 0
ip domain-lookup
no ip domain-name
no ip name-server
service telnetd
```

```
FastEthernet 0/0
ip address 10.1.5.120 255.255.0.0

exit
ip default-gateway 10.1.1.1
no ip route all

line vty 0 4
no access-class in
timeout 30
exit
```

**NME-APA#**

---

**Related Commands**

[show running-config](#) (on page 2-192)

[show startup-config](#) (on page 2-207)

## more user-log

Displays the user log on the CLI console screen.

### **more user-log**

---

#### Syntax Description

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

Authorization: admin

---

#### Examples

The following example displays the user log on the CLI console screen.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#more user-log
  <INFO>      | 01/28/97  22:29:22 | CPU #000 | Logger: Task
Initialized successfully
```

---

#### Related Commands

[logger get user-log file-name](#) (on page 2-90)

[show log](#) (on page 2-176)

## no user

Removes a specified user from the system. Use the **all** form to remove all introduced users.

**no user name** *user-name*

**no user scmp name** *scmp-name* **al**

---

### Syntax Description

*user-name* The specific user name to be removed from the system.

*scmp-name* Name of an SCMP peer device.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

Use the **scmp name all** option to remove all users managed by the specified SCMP peer device.

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example removes all users.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# no user all
NME-APA(config if)#
```

---

### Related Commands

[show interface linecard user](#) (on page 2-156)

## no user anonymous-group

Removes a specified anonymous user group from the system. Use the 'all' form to remove all anonymous user groups.

**no user anonymous-group name** *group-name*

**no user anonymous-group all**

---

|                    |                                                                           |
|--------------------|---------------------------------------------------------------------------|
| Syntax Description | <i>group-name</i> The anonymous user group to be removed from the system. |
|--------------------|---------------------------------------------------------------------------|

---

|          |                                       |
|----------|---------------------------------------|
| Defaults | This command has no default settings. |
|----------|---------------------------------------|

|               |                                  |
|---------------|----------------------------------|
| Command Modes | Linecard Interface Configuration |
|---------------|----------------------------------|

|                  |                      |
|------------------|----------------------|
| Usage Guidelines | Authorization: admin |
|------------------|----------------------|

|          |                                                                                                                                                                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Examples | <p>The following example removes all anonymous user groups.</p> <pre> <b>NME-APA</b>&gt;enable 10 Password:&lt;cisco&gt; <b>NME-APA</b>#config <b>NME-APA</b>(config)#interface linecard 0 <b>NME-APA</b>(config if)# <b>no user anonymous-group all</b> <b>NME-APA</b>(config if) </pre> |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                  |                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Related Commands | <p><a href="#">show interface linecard user anonymous-group</a> (on page 2-160)</p> <p><a href="#">no user</a> (on page 2-99)</p> |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------|

## no user mappings included-in

Use this command to remove all existing user mappings from a specified TIR or IP range.

**no user mappings included-in tp-ip-range name** *TP-IP-range-name*

**no user mappings included-in ip-range** *IP-range*

---

### Syntax Description

*TP-IP-range-name* Meaningful name assigned to this traffic processor IP range

*IP-range* IP address and mask length defining the IP range

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Use the **TP-IP-range name** parameter to remove all existing user mappings from a specified TIR.

Use the **IP-range** parameter to remove all existing user mappings from a specified IP range.

Authorization: admin

---

### Examples

The following example removes any existing user mappings from the CTMS1 TIR.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#config
```

```
NME-APA(config)#interface linecard 0
```

```
NME-APA(config if)# no user mappings included-in TP-IP-range name  
CTMS1
```

---

### Related Commands

## ping

Pings the given host to test for connectivity. The ping program sends a test message (packet) to an address and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

**ping** *host*

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>host</i> The host name or IP address of a remote station to ping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Command Modes      | Privileged EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Examples           | <p>The following example pings the host 10.1.1.201.</p> <pre> <b>NME-APA&gt;</b>enable 10 Password:&lt;<i>cisco</i>&gt; <b>NME-APA#ping</b> 10.1.1.201 pinging 10.1.1.201 ... PING 10.1.1.201: 56 data bytes 64 bytes from host (10.1.1.201): icmp_seq=0. time=0. ms 64 bytes from host (10.1.1.201): icmp_seq=1. time=0. ms 64 bytes from host (10.1.1.201): icmp_seq=2. time=0. ms 64 bytes from host (10.1.1.201): icmp_seq=3. time=0. ms ----10.1.1.201 PING Statistics---- 4 packets transmitted, 4 packets received, 0% packet loss round-trip (ms)  min/avg/max = 0/0/0 <b>NME-APA#</b> </pre> |
| Related Commands   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## pqi install file

Installs the specified *pqi* file using the installation options specified (if any). This may take up to 5 minutes.

**pqi install file** *filename* [*options options*]

---

### Syntax Description

|                 |                                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>filename</i> | The filename of the <i>pqi</i> application file to be installed.                                                                               |
| <i>options</i>  | The desired installation options. Use the <a href="#">show pqi file</a> (on page 2-179) command to display the available installation options. |

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Always run the [pqi uninstall file](#) (on page 2-105) command before installing a new *pqi* file to prevent accumulation of old files on the disk.

Authorization: admin

---

### Examples

The following example installs the application stf30519.pqi file. No options are specified.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#pqi install file stf30519.pqi
NME-APA(config if)#
```

---

### Related Commands

[show pqi file](#) (on page 2-179)

[pqi uninstall file](#) (on page 2-105)

## pqi rollback file

Reverses an upgrade of the specified *pqi* file. This may take up to 5 minutes.

**pqi rollback file** *filename*

|                    |                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>filename</i> The filename of the <i>pqi</i> application file to be rolled-back. It must be the <i>pqi</i> file that was last upgraded.                                                                                                                                                                                     |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                                                                                         |
| Command Modes      | Linecard Interface Configuration                                                                                                                                                                                                                                                                                              |
| Usage Guidelines   | Always specify the last <i>pqi</i> file that was upgraded. Use the <a href="#">show pqi last-installed</a> (on page 2-180) command.<br>Authorization: admin                                                                                                                                                                   |
| Examples           | The following example reverses the upgrade for the application using the anr100155.pqi file.<br><pre> <b>NME-APA&gt;</b>enable 10 Password:&lt;cisco&gt; <b>NME-APA#</b>config <b>NME-APA</b>(config)#interface linecard 0 <b>NME-APA</b>(config if)#<b>pqi rollback file</b> anr100155.pqi <b>NME-APA</b>(config if)# </pre> |
| Related Commands   | <a href="#">show pqi last-installed</a> (on page 2-180)                                                                                                                                                                                                                                                                       |

## pqi uninstall file

Uninstalls the specified *pqi* file. This may take up to 5 minutes.

**pqi uninstall file** *filename*

---

### Syntax Description

---

*filename* The filename of the *pqi* application file to be uninstalled. It must be the *pqi* file that was installed last.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Always specify the last *pqi* file that was installed. Use the [show pqi last-installed](#) (on page 2-180).

Always run the **pqi uninstall** command before installing a new *pqi* file to prevent accumulation of old files on the disk.

Authorization: admin

---

### Examples

The following example uninstalls the application stf30519.pqi file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#pqi uninstall file stf30519.pqi
NME-APA(config if)#
```

---

### Related Commands

[show pqi last-installed](#) (on page 2-180)

[pqi install file](#) (on page 2-103)

## pqi upgrade file

Upgrades the application using the specified *pqi* file and the upgrade options specified (if any). This may take up to 5 minutes.

**pqi upgrade file** *filename* [**options** *options*]

---

### Syntax Description

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| <i>filename</i> | The filename of the <i>pqi</i> application file to be used for the upgrade.                                                  |
| <i>options</i>  | The desired upgrade options. Use the <a href="#">show pqi file</a> (on page 2-179) command to display the available options. |

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

A given *pqi* upgrade file is suitable for upgrading only from specific previously installed *pqi* files. The upgrade procedure checks that an upgrade is possible from the currently installed *pqi* file. The upgrade procedure will be stopped with an error message if the upgrade is not possible.

Authorization: admin

---

### Examples

The following example upgrades the application using the stf30519.pqi file. No options are specified.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#pqi upgrade file stf30519.pqi
NME-APA(config if)#
```

---

### Related Commands

[show pqi file](#) (on page 2-179)  
[force failure-condition](#) (on page 2-59)

## pwd

Displays the current working directory.

### pwd

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

Authorization: admin

---

#### Examples

The following example shows the current working directory as tffs0.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#pwd  
tffs0:  
NME-APA#
```

---

#### Related Commands

[cd](#) (on page 2-23)

## queue

Sets the queue shaping.

**queue** *queue-number* **bandwidth** *bandwidth* **burst-size** *burstsize*

---

### Syntax Description

*queue-number* Queue-number from 1–4, where 4 is the highest priority (fastest). 1=BE, 2, 3=AF, and 4=EF. BE is the best effort queue, that is the lowest priority. EF is the Expedited Forwarding queue, that is the highest priority forwarding. The AF (Assured Forwarding) queues are middle-priority, with 3 being a higher priority queue, that is, packets from queue 3 are transferred faster than those in queue 2.

*bandwidth* Bandwidth measured in kbps. 0 disables packet transmission from the queue. The maximum bandwidth is determined by the line rate. Bandwidth is set in resolutions of ~140Kbps, that is rounded to the nearest multiple of approximately 140 Kbps.

*burstsize* Burst size in bytes, from 0–16000000.

---



---

### Defaults

Bandwidth = 100000K (100 Mbps)

Burst size = 8000 (8K bytes)

---

### Command Modes

FastEthernet Interface Configuration

---

### Usage Guidelines

This command is valid for a specified FastEthernet line interface only. It must be executed explicitly for each interface.

Use the [interface fastethernet](#) (on page 2-66) or command to access the configuration mode for the desired interface.

Authorization: admin

---

### Examples

The following example configures queue shaping for queue 1 for FE port #1.

```
NME-APA Module>enable 10
Password:<cisco>
NME-APA Module#config
NME-APA Module(config)#interface fastethernet 0/2
NME-APA Module(config if)#queue 1 bandwidth 20000 burstsize 1000
NME-APA Module(config if)#
```

---

### Related Commands

[bandwidth](#) (on page 2-21)

[interface fastethernet](#) (on page 2-66)

## rdr-formatter category-number

Assigns a meaningful name to a category. This category name can then be used in any **rdr-formatter** command instead of the category number. It also defines the buffer size.

Use the **no** option of this command to disassociate the name from the category. The name will then not be recognized by any CLI commands.

Use the **default** form of this command to remove all configuration (name and buffer size).

**rdr-formatter category-number** [1-4] **name** *category name*

**no rdr-formatter category-number** [1-4] **name** *category name*

**rdr-formatter category-number** [1-4] **buffer-size** *size*

**default rdr-formatter category-number** [1-4] **buffer-size**

### Syntax Description

*category name* The user-defined name to be assigned to the category.  
*size* Buffer size

### Defaults

This command has no default settings.

### Command Modes

Global Configuration

### Usage Guidelines

Authorization: admin

### Examples

The following example assigns the name “prepaid” to Category 1.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#rdr-formatter category-number 1 name prepaid
NME-APA(config)#
```

### Related Commands

[show rdr-formatter](#) (on page 2-181)  
[service rdr-formatter](#) (on page 2-124)

## rdr-formatter destination



### Note

Configuring an RDR destination entry is only for debugging purposes.

Configures an RDR destination entry. Up to four entries can be configured. Each entry must have a different priority. The entry with the highest priority is used by the RDR formatter, provided that a connection with this destination can be established. This is where the RDR-formatter sends the RDRs it produces.

Use the **no** form of the command to remove the mappings of an RDR formatter destination to categories. When all categories for a destination are removed, the entire destination is removed.

**rdr-formatter destination** *ip-address* **port** *port-number* [**category** {**name** *category name* } | {**number** [1-4]}] [**priority** *priority-value*]

**no rdr-formatter destination** *ip-address* **port** *port-number* [category {name *category name* } | {number [1-4]}]

**no rdr-formatter destination all**

### Syntax Description

*ip-address* The destination IP address.

*port-number* The destination port number.

*category* (Optional) Use this parameter to assign a priority to a particular category for this destination.

*category name* (Optional) User-defined name that identifies the category

*number* (Optional) Use this parameter to identify the category by number (1 to 4).

*priority-value* The priority of the destination. The priority value may be any number between 1 (lowest) to 100 (highest).

### Defaults

This command has no default settings.

### Command Modes

Global Configuration

### Usage Guidelines

The category may be identified by either name or number.

Assign a high priority to send RDRs from the specified category to this destination. Assign a low priority if RDRs from the specified category should not be sent to this destination.

For the first entry, if no priority is set, the highest priority is automatically assigned.

For all subsequent entries, the priority must be explicitly defined.

It is also possible to assign a different priority to each category for each destination. If no category is specified, the same priority is assigned to all categories for that destination.

Use the **all** keyword with the **no** form of the command to remove all of the configured RDR-formatter categories from the specified destination, thus removing the destination itself.

Authorization: admin

---

### Examples

The following examples illustrate the use of the **RDR-formatter destination** command:

#### EXAMPLE 1:

The following example configures an RDR-formatter destination with the default priority (highest) to be used by all categories.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#rdr-formatter destination 10.1.1.205 port 33000
NME-APA(config)#
```

#### EXAMPLE 2:

The following example configures an RDR-formatter destination for two categories with a different priority for each category. This configuration will send RDRs from category 2 to this destination, but generally not RDRs from category 1.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#rdr-formatter destination 10.1.1.206 port 34000
category number 1 priority 10 category number 2 priority 90
NME-APA(config)#
```

---

### Related Commands

[show rdr-formatter destination](#) (on page 2-184)

[service rdr-formatter](#) (on page 2-124)

## rdr-formatter forwarding-mode

Defines the mode in which the RDR formatter will send the RDRs to the destinations.

**rdr-formatter forwarding-mode** *mode*

### Syntax Description

*mode* Settings: **redundancy**, **multicast**, **simple-load-balancing** as described in the Valid Mode Settings table in the Usage Guidelines.

### Defaults

Default *mode* = **redundancy**

### Command Modes

Global Configuration

### Usage Guidelines

Table 2-1 Valid Mode Settings

|                              |                                                            |
|------------------------------|------------------------------------------------------------|
| <b>redundancy</b>            | All RDRs are sent only to the primary (active) connection. |
| <b>multicast</b>             | All RDRs are sent to all destinations.                     |
| <b>simple-load-balancing</b> | Not currently supported                                    |

Authorization: admin

### Examples

The following example sets the RDR formatter mode to “**redundancy**”.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#rdr-formatter forwarding-mode redundancy
NME-APA(config)#
```

### Related Commands

[show rdr-formatter forwarding-mode](#) (on page 2-186)

## rdr-formatter history-size

Configures the size of the history buffer.

This command is currently not supported.

**rdr-formatter history-size** *size*

---

### Syntax Description

---

*size*      Size of the history buffer in bytes. Must be = 0 only (default)

---

---

### Defaults

Default size = 0

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Do not change the size of the history buffer from the default value.

Since currently only RDRv1 is supported, the size of the history buffer must be zero bytes, even though the system will accept a command specifying a larger size

Authorization: admin

---

### Examples

---

### Related Commands

[show rdr-formatter history-size](#) (on page 2-187)

## rdr-formatter rdr-mapping

Adds a dynamic RDR mapping to a category or removes one from a category.

Use the no form of this command to remove an existing mapping.

**rdr-formatter rdr-mapping (tag-id tag number category-number category number)**

**no rdr-formatter rdr-mapping (tag-id tag number category-number category number)**

|                    |                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <p><i>tag number</i> The complete 32 bit value given as an hexadecimal number. The RDR tag must be already configured in the Formatter by the application.</p> <p><i>category number</i> Number of the category (1-4) to which to map the RDR tag</p> |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Defaults This command has no default settings.

Command Modes Global Configuration

Usage Guidelines The configuration of categories to RDR tags is done by adding and removing mappings. You can add a mapping of RDR tag to a category and remove a mapping, including the default mapping. If the table already contains a mapping with the same tag and category number, an error is issued and nothing is done.

If only one category is left configured for a certain tag, it cannot be removed.

Authorization: admin

Examples The following examples illustrate how to add and remove mappings, and how to restore default mapping

### EXAMPLE 1

This example shows how to add a mapping to a category.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#rdr-formatter rdr-mapping tag-id 0xf0f0f000
category-number 1
NME-APA(config)#
```

**EXAMPLE 2**

This example shows how to restore the default mapping for a specified RDR tag.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#default rdr-formatter rdr-mapping tag-id
0xf0f0f000
NME-APA(config)#
```

---

**Related Commands**

[show rdr-formatter rdr-mapping](#) (on page 2-188)

## reload

Reboots the NME-APA module.

### reload



#### Warning

In order not to lose the current configuration, use the **copy running-config-all startup-config-all** command before using the **reload** command.

#### Syntax Description

This command has no arguments or keywords.

#### Defaults

This command has no default settings.

#### Command Modes

Privileged EXEC

#### Usage Guidelines

Authorization: admin

#### Examples

The following example shows backing up of the configuration and performing a system reboot.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#copy running-config-all startup-config-all
```

```
NME-APA#reload
```

```
Are you sure? Y
```

```
The system is about to reboot, this will end your CLI session
```

#### Related Commands

[copy running-config startup-config](#) (on page 2-45)

## rename

Changes the file name to the specified name.

**rename** *existing-file-name* *new-file-name*

---

### Syntax Description

*existing-file-name* The original name of the file.

*new-file-name* The new name of the file.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example changes the name of file test1.pkg to test3.pkg.

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#rename test1.pkg test3.pkg
```

```
NME-APA#
```

---

### Related Commands

**rmdir**

Removes an empty directory.

To remove a directory that is not empty, use the [delete](#) (on page 2-50) command with the recursive switch.

**rmdir** *directory-name*

|                    |                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>directory-name</i> The name of the directory to be removed.                                                                                                                             |
| Defaults           | This command has no default settings.                                                                                                                                                      |
| Command Modes      | Privileged EXEC                                                                                                                                                                            |
| Usage Guidelines   | <p>You can only remove an empty directory. Use the <a href="#">dir</a> (on page 2-51) command to verify that no files are listed in this directory.</p> <p>Authorization: admin</p>        |
| Examples           | <p>The following example deletes the <b>code</b> directory.</p> <pre><b>NME-APA&gt;</b>enable 10 <b>NME-APA&gt;</b>password: &lt;cisco&gt; <b>NME-APA#</b>rmdir code <b>NME-APA#</b></pre> |
| Related Commands   | <p><a href="#">dir</a> (on page 2-51)</p> <p><a href="#">delete</a> (on page 2-50)</p>                                                                                                     |

## script capture

Begins the recording of a script. It tracks all commands typed until the *script stop* (on page 2-122) command is used.

Use this command to capture a sequence of repeated commands into a file for the purpose of executing the commands again.

Use the *script stop* (on page 2-122) command to stop capturing the script.

**script capture** *script-file-name*

---

### Syntax Description

---

*script-file-name* The name of the output file where the script is stored.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example shows the script capture for the script1.txt.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#script capture script1.txt  
NME-APA#cd log  
NME-APA#cd ..  
NME-APA#pwd  
NME-APA#script stop
```

---

### Related Commands

*script stop* (on page 2-122)

## script print

Displays a script file.

**script print** *script-file-name*

---

### Syntax Description

*script-file-name* The name of the file containing the script.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example prints the commands captured in script1.txt.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#script print script1.txt
cd log
cd ..
pwd
script stop
NME-APA#
```

---

### Related Commands

[script capture](#) (on page 2-119)

[script run](#) (on page 2-121)

## script run

Runs a script. The script may be created using the **script capture** command, or it may be created as a text file containing the appropriate commands.

**script run** *script-file-name* [**halt**]

---

### Syntax Description

*script-file-name* The name of the file containing the script.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Use this command to run a script that you have previously created using the **script capture** command.

Use the **halt** keyword to break script on errors.

Authorization: admin

---

### Examples

The following example runs the script named *monitor.txt*, which contains the following commands to enable the generation of the real-time user usage RDRs for the specified users:

```
configure
interface linecard 0
user name Jerry property monitor value 1
user name George property monitor value 1
user name Elaine property monitor value 1
user name Kramer property monitor value 1

NME-APA>enable 10
Password:<cisco>
NME-APA#script run monitor.txt
NME-APA#configure
NME-APA(config)#interface linecard 0
NME-APA(config if)#user name Jerry property monitor value 1
NME-APA(config if)#user name George property monitor value 1
NME-APA(config if)#user name Elaine property monitor value 1
NME-APA(config if)#user name Kramer property monitor value 1
NME-APA(config if)#
```

---

### Related Commands

[script capture](#) (on page 2-119)

[script print](#) (on page 2-120)

## script stop

Stops script capture. Used in conjunction with the *script capture* (on page 2-119) command, it marks the end of a script being recorded.

### script stop

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

Authorization: admin

---

#### Examples

The following example stops the capturing of a script.

```
NME-APA>enable 10
NME-APA>Password:<cisco>
NME-APA#script capture script1.txt
NME-APA#cd log
NME-APA#cd ..
NME-APA#pwd
NME-APA#script stop
NME-APA#
```

---

#### Related Commands

*script capture* (on page 2-119)

## service password-encryption

Enables password encryption, so that the password remains secret when the configuration file is displayed. Use the **no** form of this command to disable password encryption.

**service password-encryption**

**no service password-encryption**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | This command has no arguments or keywords.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Defaults           | Disabled (no encryption)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Usage Guidelines   | <p>Passwords that were configured in an encrypted format are not deciphered when password encryption is disabled.</p> <p>Authorization: admin</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Examples           | <p>The following example shows the effect of enabling password encryption.</p> <pre> <b>NME-APA&gt;enable 10</b> Password:&lt;cisco&gt; <b>NME-APA#config</b> <b>NME-APA(config)#enable password abcd</b> <b>NME-APA(config)#do more running-config</b> #This is a general configuration file (running-config). #Created on 10:20:57  ISR  TUE  July  3  2001 ... enable password level 10 0 "abcd" ... <b>NME-APA(config)#service password-encryption</b> <b>NME-APA(config)#do more running-config</b> #This is a general configuration file (running-config). #Created on 10:21:12  ISR  TUE  July  3  2001 ... service password-encryption enable password level 10 0 "e2fc714c4727ee9395f324cd2e7f331f" ... <b>NME-APA(config)#</b> </pre> |
| Related Commands   | <a href="#">enable password</a> (on page 2-55)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## service rdr-formatter

Enables/disables the RDR-formatter. The RDR-formatter is the element that formats the reports of events produced by the linecard and sends them to an external data collector.

Use the **no** keyword of this command to disable the RDR-formatter.

**service rdr-formatter**

**no service rdr-formatter**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | This command has no arguments or keywords                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Defaults           | Enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Examples           | <p>The following examples illustrate the use of the <b>service rdr-formatter</b> command:</p> <p><b>EXAMPLE 1:</b></p> <p>The following example enables the RDR-formatter.</p> <pre>NME-APA&gt;enable 10 Password:&lt;cisco&gt; NME-APA#config NME-APA(config)#service rdr-formatter NME-APA(config)#</pre> <p><b>EXAMPLE 2:</b></p> <p>The following example disables the RDR-formatter.</p> <pre>NME-APA(config)#no service rdr-formatter NME-APA(config)#</pre> |
| Related Commands   | <p><a href="#">show rdr-formatter enabled</a> (on page 2-185)</p> <p><a href="#">rdr-formatter category-number</a> (on page 2-109)</p> <p><a href="#">rdr-formatter destination</a> (on page 2-110)</p>                                                                                                                                                                                                                                                            |

## service telnetd

Enables/disables Telnet daemon. Use the **no** form of this command to disable the daemon preventing new users from accessing the NME-APA module via Telnet.

**service telnetd**

**no service telnetd**

---

### Syntax Description

This command has no arguments or keywords,

---



---

### Defaults

Telnet daemon enabled

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following examples illustrate the use of the **service telnetd** command:

**EXAMPLE 1:**

The following example enables the Telnet daemon.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#service telnetd
NME-APA(config)#
```

**EXAMPLE 2:**

The following example disables the Telnet daemon.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#no service telnetd
NME-APA(config)#
```

---

### Related Commands

[show telnet status](#) (on page 2-213)

[telnet](#) (on page 2-236)

## setup

Invokes the setup utility, which is a dialog, or series of questions, that guides the user through the basic configuration process. This utility runs automatically upon initial connection to the local terminal. The utility may also be invoked explicitly to make changes to the system configuration.

### setup

Following is a brief list of the parameters configured via the setup command:

- Host ID parameters: hostname
- Passwords: admin/root password, password encryption
- Anonymous User Groups: anonymous user group name, anonymous user group IP range
- Time settings: time zone, offset from UTC, local time and date
- SNMP configuration: multicast client, unicast server, unicast query interval
- SNMP configuration:

Define the following:

- GET community names (up to 20)
- SET community names (up to 20)
- trap managers (up to 20): IP address, community string, version
- name of system manager

For a complete description of the command, see the *Cisco NME-APA User Guide*.

### Syntax Description

The setup command does not include parameters in the usual sense of the word. However, the setup utility questions prompt for many global configuration parameters. Following is a table listing all parameters for which values may be requested by the setup dialog.

The table in the *Usage Guidelines* lists all the parameter values that are necessary to complete the initial configuration. It is recommended that you obtain all these values before beginning the setup.

### Defaults

### Command Modes

Privileged EXEC

### Usage Guidelines

**Table 2-2 Setup Command Parameters**

| Parameter | Definition                                                                             |
|-----------|----------------------------------------------------------------------------------------|
| hostname  | Character string used to identify the NME-APA module. Maximum length is 20 characters. |

| Parameter                          | Definition                                                                                                                                                 |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| admin password                     | Admin level password.<br>Character string from 4-100 characters beginning with an alpha character.                                                         |
| root password                      | Root level password.<br>Character string from 4-100 characters beginning with an alpha character.                                                          |
| password encryption status         | Enable or disable password encryption?                                                                                                                     |
| User Anonymous Group Settings      |                                                                                                                                                            |
| user anonymous group name          | Character string used to identify the anonymous users group.                                                                                               |
| user anonymous group IP range      | IP range of the anonymous users group in the format A.B.C.D/E                                                                                              |
| Time Settings                      |                                                                                                                                                            |
| time zone name and offset          | Standard time zone abbreviation and minutes offset from UTC.                                                                                               |
| local time and date                | Current local time and date. Use the format:<br>00:00:00 1 January 2002                                                                                    |
| SNTP Configuration                 |                                                                                                                                                            |
| broadcast client status            | Set the status of the SNTP broadcast client.<br>If enabled, the NME-APA will synchronize its local time with updates received from SNTP broadcast servers. |
| unicast query interval             | Interval in seconds between unicast requests for update (64 – 1024)                                                                                        |
| unicast server IP address          | IP address of the SNTP unicast server.                                                                                                                     |
| SNMP Configuration                 |                                                                                                                                                            |
| SNMP agent status                  | Enable or disable SNMP management.                                                                                                                         |
| GET community names                | Community strings to allow GET access and associated ACLs (maximum 20).                                                                                    |
| SET community names                | Community strings to allow SET access and associated ACLs (maximum 20).                                                                                    |
| trap managers (maximum 20)         | Trap manager IP address, community string, and SNMP version.                                                                                               |
| Authentication Failure trap status | Sets the status of the Authentication Failure traps.                                                                                                       |
| enterprise traps status            | Sets the status of the enterprise traps.                                                                                                                   |
| system administrator               | Name of the system administrator.                                                                                                                          |

Authorization: admin

### Examples

The following example runs the setup utility.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#setup
```

## --- System Configuration Dialog ---

At any point you may enter a question mark '?' followed by 'Enter' for help.

Use ctrl-C to abort configuration dialog at any prompt.

Use ctrl-Z to jump to the end of the configuration dialog at any prompt.

Default settings are in square brackets '['].

Would you like to continue with the System Configuration Dialog?  
[yes/no]: **y**

---

Related Commands

## show calendar

Displays the time maintained by the real-time system calendar clock.

### show calendar

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the current system calendar.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show calendar  
12:50:03 GMT MON November 13 2005  
NME-APA>
```

---

#### Related Commands

[calendar set](#) (on page 2-22)

## show clock

Displays the time maintained by the system clock.

### show clock

---

#### Syntax Description

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the current system clock.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show clock  
12:50:03 GMT MON November 13 2005  
NME-APA>
```

---

#### Related Commands

[clock set](#) (on page 2-34)

## show failure-recovery operation-mode

Displays the operation mode to apply after boot resulted from failure.

### show failure-recovery operation-mode

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example displays the failure recovery operation mode:

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show failure-recovery operation-mode  
System Operation mode on failure recovery is: operational  
NME-APA>
```

---

**Related Commands**

[failure-recovery operation-mode](#) (on page 2-50)

## show hostname

Displays the currently configured hostname.

### show hostname

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows that NME-APA1 is the current hostname.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show hostname  
NME-APA1  
NME-APA>
```

---

#### Related Commands

[hostname](#) (on page 2-65)

## show hosts

Displays the default domain name, the address of the name server, and the content of the host table.

### show hosts

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the domain and hosts configured.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show hosts  
Default domain is cisco.com  
Name/address lookup uses domain service  
Name servers are 10.1.1.60, 10.1.1.61  
Host                Address  
----                -  
PC85                10.1.1.61  
NME-APA>
```

---

**Related Commands**

[hostname](#) (on page 2-65)

[ip domain-name](#) (on page 2-71)

[ip name-server](#) (on page 2-78)

## show interface fastethernet

Displays the details of a FastEthernet Interface.

**show interface fastethernet** *slot-number/interface-number* [**counters** [*direction*]]**duplex|speed|queue** *queue-number*

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*interface-number* The FastEthernet interface number.

*direction* Optional direction specification, to show only counters of a specific direction. Use **in** or **out**.

*queue-number* Number of queue, in the range 0-3.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

The following keywords are relevant to the line interfaces (1 – 2) of the NME-APA module:

- The **duplex** keyword displays the configured and actual duplex mode of the specified interface.
- The **speed** keyword displays the configured and actual speed of the specified interface.
- The **counters** keyword displays the values of counters for the specified line interface.
- The **queue** keyword displays the bandwidth and burst size of the specified queue in the specified line interface.

Authorization: viewer

---

### Counter Definitions

Following are definitions of the counters displayed in the output of this command.

In total octets: Total number of inbound octets

In good unicast packets: Total number good inbound unicast packets

In good multicast packets: Total number of good inbound multicast packets

In good broadcast packets: Total number of good inbound broadcast packets

In packets discarded: Total number of inbound discarded packets

In packets with CRC/Alignment error: Total number of inbound packets with CRC or alignment errors

In undersized packets: Total number of inbound undersized packets

In oversized packets: Total number of inbound oversized packets

Out unicast packets: Total number of outbound unicast packets  
Out non unicast packets: Total number of outbound non-unicast packets  
Out packets discarded: Total number of outbound discarded packets

---

**Examples**

The following examples illustrate the use of the **show interface FastEthernet** command:

**EXAMPLE 1:**

The following example shows the FastEthernet details for a line interface.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show interface fastethernet 0/1  
Configured speed: auto, configured duplex: auto  
AutoNegotiation is On, link is Up, actual speed: 100Mb/s, actual  
duplex: full  
Bandwidth: 100000 Kbps, Burst-size: 5000 bytes  
NME-APA>
```

**EXAMPLE 2:**

The following example shows the FastEthernet interface counters.

```
NME-APA>show interface fastethernet 0/1 counters  
In total octets: 191520  
In good unicast packets: 560  
In good multicast packets: 0  
In good broadcast packets: 0  
In packets discarded: 0  
In packets with CRC/Alignment error: 0  
In undersized packets: 0  
In oversized packets: 0  
Out total octets: 0  
Out unicast packets: 0  
Out non unicast packets: 0  
Out packets discarded: 0  
NME-APA>
```

**EXAMPLE 3:**

The following example shows the FastEthernet interface duplex mode configuration and status.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show interface fastethernet 0/1 duplex  
Configured duplex: auto  
AutoNegotiation is On, link is Up, actual duplex: half  
NME-APA>
```

**EXAMPLE 4:**

The following example shows the FastEthernet interface speed configuration and status.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface fastethernet 0/1 speed
Configured speed: auto
AutoNegotiation is On, link is Up, actual speed: 100
NME-APA>
```

**EXAMPLE 5:**

The following example shows the FastEthernet interface queue number 1.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface fastethernet 0/1 queue 3
Bandwidth: 100000 Kbps, Burst-size: 8000 bytes
NME-APA>
```

Related Commands [interface fastethernet](#) (on page 2-66)

## show interface linecard

Displays information for a specific linecard Interface.

**show interface linecard** *slot-number*

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following example shows how to use this command.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0
```

```
The application assigned to slot 0 is /tffs0/app/eng30102.sli
```

```
Silent is off
```

```
Configured shutdown is off
```

```
Shutdown due to sm-connection-failure is off
```

```
Resulting current shutdown state is off
```

```
NME-APA>
```

---

### Related Commands

[interface linecard](#) (on page 2-67)

## show interface linecard application

Displays the name of the application loaded on the Linecard Interface.

### show interface linecard *slot-number* application

---

#### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the currently loaded application.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 application
/tffs0/app/eng30102.sli
NME-APA>
```

---

#### Related Commands

## show interface linecard attack-detector

Displays the configuration of the specified attack detector.

The following information is displayed:

- Protocol
- Side — Whether the attack detector applies to attacks originating at the user or network side.
- Direction — Whether the attack detector applies to single sided or dual sided attacks.
- Action to take if an attack is detected.
- Thresholds:
  - open-flows-rate — Default threshold for rate of open flows (new open flows per second).
  - suspected-flows-rate — Default threshold for rate of suspected DDoS flows (new suspected flows per second).
  - suspected-flows-ratio — Default threshold for ratio of suspected flow rate to open flow rate.
- User notification — enabled or disabled.
- Alarm: sending an SNMP trap enabled or disabled.

**show interface linecard** *slot-number* **attack-detector** [**default|all**]

**show interface linecard** *slot-number* **attack-detector** *attack-detector*

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*attack-detector* The number of the specific attack detector to be displayed.

**all** Displays the configuration of all existing attack detectors

**default** Displays the default attack detector configuration.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Use the **all** keyword to display the configuration of all existing attack detectors.

Use the **default** keyword to display default attack detector configuration.

Authorization: viewer

## Examples

The following examples illustrate the **show interface linecard attack-detector** command:

**EXAMPLE 1:**

The following example displays the configuration of attack detector number 3.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 attack-detector 3
```

```
Detector #3:
```

```
Comment: 'Sample'
```

```
Access-list: 1
```

```
Effective only for TCP port(s) 21,23,80
```

```
Effective for all UDP ports
```

| Protocol | Side  | Direction   | Action | Thresholds |                |       |
|----------|-------|-------------|--------|------------|----------------|-------|
| Sub-     | Alarm |             |        | Open flows | Ddos-Suspected |       |
| flows    | notif |             |        | rate       | rate           | ratio |
| -----    | ----  | -----       | ----   | -----      | -----          | ----- |
| TCP      | net.  | source-only |        |            |                |       |
| TCP      | net.  | dest-only   |        |            |                |       |
| TCP      | sub.  | source-only |        |            |                |       |
| TCP      | sub.  | dest-only   |        |            |                |       |
| TCP      | net.  | source+dest |        |            |                |       |
| TCP      | sub.  | source+dest |        |            |                |       |
| TCP+port | net.  | source-only | Block  |            |                |       |
|          | Yes   |             |        |            |                |       |
| TCP+port | net.  | dest-only   |        |            |                |       |
| TCP+port | sub.  | source-only | Block  |            |                |       |
|          | Yes   |             |        |            |                |       |
| TCP+port | sub.  | dest-only   |        |            |                |       |
| TCP+port | net.  | source+dest |        |            |                |       |
| TCP+port | sub.  | source+dest |        |            |                |       |

|          |                    |
|----------|--------------------|
| UDP      | net.   source-only |
|          |                    |
| UDP      | net.   dest-only   |
|          |                    |
| UDP      | sub.   source-only |
|          |                    |
| UDP      | sub.   dest-only   |
|          |                    |
| UDP      | net.   source+dest |
|          |                    |
| UDP      | sub.   source+dest |
|          |                    |
| UDP+port | net.   source-only |
|          |                    |
| UDP+port | net.   dest-only   |
|          |                    |
| UDP+port | sub.   source-only |
|          |                    |
| UDP+port | sub.   dest-only   |
|          |                    |
| UDP+port | net.   source+dest |
|          |                    |
| UDP+port | sub.   source+dest |
|          |                    |
| ICMP     | net.   source-only |
|          |                    |
| ICMP     | net.   dest-only   |
|          |                    |
| ICMP     | sub.   source-only |
|          |                    |
| Yes      |                    |
| ICMP     | sub.   dest-only   |
|          |                    |
| other    | net.   source-only |
|          |                    |
| other    | net.   dest-only   |
|          |                    |
| other    | sub.   source-only |
|          |                    |
| other    | sub.   dest-only   |
|          |                    |

Empty fields indicate that no value is set and configuration from the default attack detector is used.

**NME-APA>**

**EXAMPLE 2:**

The following example displays the configuration of the default attack detector.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 attack-detector default
```

| Protocol                                  | Side  | Direction   | Action | Thresholds |                |       |
|-------------------------------------------|-------|-------------|--------|------------|----------------|-------|
| Sub-                                      | Alarm |             |        | Open flows | Ddos-Suspected |       |
| Flows                                     | notif |             |        | rate       | rate           | ratio |
| ----- ----- ----- ----- ----- ----- ----- |       |             |        |            |                |       |
| - ----- -----                             |       |             |        |            |                |       |
| TCP                                       | net.  | source-only | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP                                       | net.  | dest.-only  | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP                                       | sub.  | source-only | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP                                       | sub.  | dest.-only  | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP                                       | net.  | source+dest | Report | 100        | 50             | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP                                       | sub.  | source+dest | Report | 100        | 50             | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP+port                                  | net.  | source-only | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP+port                                  | net.  | dest.-only  | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP+port                                  | sub.  | source-only | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP+port                                  | sub.  | dest.-only  | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP+port                                  | net.  | source+dest | Report | 100        | 50             | 50    |
| No                                        | No    |             |        |            |                |       |
| TCP+port                                  | sub.  | source+dest | Report | 100        | 50             | 50    |
| No                                        | No    |             |        |            |                |       |
| UDP                                       | net.  | source-only | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| UDP                                       | net.  | dest.-only  | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| UDP                                       | sub.  | source-only | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| UDP                                       | sub.  | dest.-only  | Report | 1000       | 500            | 50    |
| No                                        | No    |             |        |            |                |       |
| UDP                                       | net.  | source+dest | Report | 100        | 50             | 50    |
| No                                        | No    |             |        |            |                |       |
| UDP                                       | sub.  | source+dest | Report | 100        | 50             | 50    |
| No                                        | No    |             |        |            |                |       |

|          |                    |        |      |          |
|----------|--------------------|--------|------|----------|
| UDP+port | net.   source-only | Report | 1000 | 500   50 |
| No       | No                 |        |      |          |
| UDP+port | net.   dest.-only  | Report | 1000 | 500   50 |
| No       | No                 |        |      |          |
| UDP+port | sub.   source-only | Report | 1000 | 500   50 |
| No       | No                 |        |      |          |
| UDP+port | sub.   dest.-only  | Report | 1000 | 500   50 |
| No       | No                 |        |      |          |
| UDP+port | net.   source+dest | Report | 100  | 50   50  |
| No       | No                 |        |      |          |
| UDP+port | sub.   source+dest | Report | 100  | 50   50  |
| No       | No                 |        |      |          |
| ICMP     | net.   source-only | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| ICMP     | net.   dest.-only  | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| ICMP     | sub.   source-only | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| ICMP     | sub.   dest.-only  | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| other    | net.   source-only | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| other    | net.   dest.-only  | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| other    | sub.   source-only | Report | 500  | 250   50 |
| No       | No                 |        |      |          |
| other    | sub.   dest.-only  | Report | 500  | 250   50 |
| No       | No                 |        |      |          |

**NME-APA>**

#### Related Commands

[attack-detector](#) (on page 2-11)

[attack-detector default](#) (on page 2-9)

[attack-detector <number>](#) (on page 2-12)

## show interface linecard attack-filter

Displays the attack filtering configuration.

**show interface linecard** *slot-number* **attack-filter** [*option*]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*option* See Usage Guidelines for the list of options.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Following is a list of options that may be displayed:

- **query IP configured:** displays the configured threshold values and action as follows:
  - **query single-sided IP** *ip-address* **configured:** displays the configured threshold values and action for attack detection for a specified IP address (single-sided detection)
  - **query dual-sided source-IP** *ip-address1* **dest** *ip-address2* **configured:** displays the configured threshold values and action for attack detection between two specified IP addresses (dual-sided detection)
  - **dest-port** *port#:* displays the configured threshold values and action for the specified port. You can include this argument with both single-sided and dual-sided queries.
- **query IP current:** displays the current counters for a specified attack detector for all protocols and attack directions as follows:
  - **query single-sided IP** *ip-address* **current:** displays the current counters for attack detection for a specified IP address (single-sided detection)
  - **query dual-sided source-IP** *ip-address1* **dest** *ip-address2* **current:** displays the current counters for attack detection between two specified IP addresses (dual-sided detection)
  - **dest-port** *port#:* displays the configured threshold values and action for the specified port. You can include this argument with both single-sided and dual-sided queries.
- **current-attacks:** displays all currently handled attacks
- **counters:** displays all attack detection counterd
- **dont-filter:** displays all existing stopped attack filters
- **force-filter:** displays all existing forced attack filters
- **user-notification ports:** displays the list of user-notification ports
- **user-notification redirect:** displays the configuration of user-notification redirection, such as the configured destination and dismissal URLs, and allowed hosts.

Authorization: viewer

---

**Examples**

The following examples illustrate the use of the **show interface linecard attack-filter** command.

**EXAMPLE 1:**

The following example displays the configuration of attack detection between two specified IP addresses (dual-sided) for destination port 101.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 attack-filter query dual-sided
source-IP 10.10.10.10 dest 10.10.10.145 dest-port 101 configured
```

```
NME-APA>
```

**EXAMPLE 2:**

The following example displays all existing forced attack filters.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 attack-filter force-filter
No force-filter commands are set for slot 0
NME-APA>
```

**EXAMPLE 3:**

The following example displays the user notification ports.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 attack-filter user-notification
ports
Configured User notification ports: 100
NME-APA>
```

---

**Related Commands**

[attack-filter \(Linecard Interface Configuration\)](#) (on page 2-16)

[attack-filter \(Privileged Exec\)](#) (on page 2-18)

## show interface linecard counters

Displays the Linecard Interface counters.

**show interface linecard** *slot-number* **counters** [**bandwidth**] [**cpu-utilization**] [**cpu-history**] [**all-active-users**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---

### Defaults

This command has no default settings.

### Command Modes

User Exec

### Usage Guidelines

Specify any of the optional keywords to display only the desired counters.

Authorization: viewer

### Example

The following example shows the hardware counters for the Linecard Interface.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 counters
DP packets in: 100
DP packets out: 100
DP IP packets in: 90
DP Non-IP packets: 10
DP IP packets with CRC error: 0
DP IP packets with length error: 0
DP IP broadcast packets: 10
DP IP fragmented packets: 0
DP IP packets with TTL=0 error: 0
DP Non TCP/UDP packets: 10
DP TCP/UDP packets with CRC error: 0
FF counter #0: 0
FF counter #1: 0
FF counter #2: 0
FF counter #3: 0
...
NME-APA>
```

---

### Related Commands

[clear interface linecard](#) (on page 2-25)

## show interface linecard duplicate-packets-mode

Displays the currently configured duplicate packets mode.

**show interface linecard** *slot-number* **duplicate-packets-mode**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

Authorization: viewer

---

### Usage Guidelines

---

### Example

The following example illustrates the use of the **show interface linecard duplicate-packets-mode** command:

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 duplicate-packets-mode
```

```
Packet duplication of flows due to Delay Sensitive <bundles> is enabled
```

```
Packet duplication of flows due to No-Online-Control <set-flow> is enabled
```

```
Packet duplication of flows due to No-Online-Control <set-flow> ratio percent is 70
```

```
Packet duplication in case of shortage is enabled
```

```
NME-APA>
```

---

### Related Commands

## show interface linecard flow-open-mode

Displays the currently configured flow open mode.

**show interface linecard *slot-number* flow-open-mode**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

Authorization: viewer

---

### Usage Guidelines

---

### Example

The following example illustrates the use of the **show interface linecard flow-open-mode** command:

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 flow-open-mode
```

```
Enhanced flow open mode is disabled
```

```
NME-APA>
```

---

### Related Commands

## show interface linecard link mode

Displays the configured Linecard Interface link mode.

**show interface linecard** *slot-number* **link mode**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following example shows the configured link mode for the Linecard Interface.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 link mode
Link mode on port1-port2
Current link mode is           :forwarding
Actual link mode on active is   :forwarding
Actual link mode on failure is  :monopath-bypass
NME-APA>
```

---

### Related Commands

[link mode](#) (on page 2-84)

## show interface linecard link-to-port-mappings

Displays the link ID to port ID mappings.

**show interface linecard *slot-number* link-to-port-mappings**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Example

The following example shows the link ID to port ID mapping for the Linecard Interface.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 link-to-port-mappings
Link Id      | Upstream Port <Out> | Downstream Port <Out>
-----
0            | 0/2                 | 0/1
NME-APA>
```

---

### Related Commands

## show interface linecard shutdown

Displays the current shutdown state.

**show interface linecard** *slot-number* **shutdown**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following example shows the linecard Interface silent mode.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show interface linecard 0 shutdown  
  
NME-APA>
```

---

### Related Commands

## show interface linecard silent

Displays the current Linecard Interface silent state. When the silent state is Off, the linecard events reporting function is enabled.

**show interface linecard *slot-number* silent**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following example shows the Linecard Interface silent mode.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 silent
off
NME-APA>
```

---

### Related Commands

[silent](#) (on page 2-221)

## show interface linecard tos-marking table

Displays the current linecard TOS marking table.

**show interface linecard** *slot-number* **tos-marking table**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following example shows the ToS marking table:

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 tos-marking table
```

|        |     | BE  | AF1  | AF2  | AF3  | AF4  | FE   |
|--------|-----|-----|------|------|------|------|------|
| green  | 0x0 | 0xa | 0x12 | 0x1a | 0x22 | 0x2e |      |
| yellow |     | 0x0 | 0xc  | 0x14 | 0x1c | 0x24 | 0x2e |
| red    | 0x0 | 0xe | 0x16 | 0x1e | 0x24 | 0x2e |      |

```
NME-APA>
```

---

### Related Commands

[tos-marking set-table-entry](#) (on page 2-239)

## show interface linecard traffic-counter

Displays the specified traffic counter.

**show interface linecard** *slot-number* **traffic-counter** *name* [**all**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*name* Name of the traffic counter to be displayed.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Use the **all** keyword to display all traffic counters.

Authorization: viewer

---

### Examples

The following example displays information for all existing traffic counters.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 traffic-counter all
```

```
Counter 'cnt' value: 0 packets. Rules using it: None.
```

```
Counter 'cnt2' value: 1284 packets. Rules using it: Rule2.
```

```
2 counters listed out of 32 available.
```

```
NME-APA>
```

---

### Related Commands

[traffic-counter](#) (on page 2-241)

[clear interface linecard traffic-counter](#) (on page 2-26)

## show interface linecard traffic-rule

Displays the specified traffic rule configuration.

**show interface linecard** *slot-number* **traffic-rule name** *name* | **tunnel-id-mode** | **all**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*name* Name of the traffic rule to be displayed.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Use the **all** keyword to display all traffic counter rules.

Use the **tunnel-id-mode** to display all rules defined in tunnel-id-mode.

Authorization: viewer

---

### Examples

The following example displays traffic rule information.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 traffic-rule name Rule1
```

```
0 rules listed out of 127 available.
```

```
NME-APA>
```

---

### Related Commands

[traffic-rule](#) (on page 2-243)

## show interface linecard user

Displays names of users or the number of users meeting one of the following specified criteria:

- Having a value of a user property that is equal to, larger than, or smaller than a specified value
- Having a user name that matches a specific prefix
- Having a user name that matches a specific suffix

**show interface linecard** *slot-number* **user** [amount] [**prefix** *prefix*] [**suffix** *suffix*] [**property** *propertyname* **equals|bigger-than|less-than** *property-val*] [**all-names**]

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <p><i>slot-number</i> The number of the identified slot. Enter a value of 0.</p> <p><i>prefix</i> The desired user name prefix to match.</p> <p><i>suffix</i> The desired user name suffix to match.</p> <p><i>propertyname</i> The name of the user property to match.</p> <p><i>property-val</i> The value of the specified user property. Specify whether to search for values equal to, greater than, or less than this value.</p> |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Defaults This command has no default settings.

Command Modes User Exec

Usage Guidelines Use the **amount** keyword to display the number of users meeting the criteria rather than listing actual user names.

Use the **all-names** keyword to display the names of all users currently in the NME-APA module user database.

Authorization: viewer

Examples The following examples illustrate the use of this command.

### EXAMPLE 1

Following is an example that lists the number of users with the prefix 'gold' in the user name

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user amount prefix gold
There are 40 users with name prefix 'gold'.
NME-APA>
```

**EXAMPLE 2**

Following is an example that lists all users currently in the NME-APA module users database.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user all-names
There are 8 users in the database.
john_doe
mary_smith
david_jones
betty_peters
bill_jackson
jane_doe
bob_white
andy_black
NME-APA>
```

---

**Related Commands**

[user name property](#) (on page 2-251)

## show interface linecard user aging

Displays the user aging configuration for the specified type of user (anonymous or introduced).

**show interface linecard** *slot-number* **user aging** [**anonymous**|**introduced**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Use the **anonymous** keyword to display the user aging configuration for anonymous users.

Use the **introduced** keyword to display the user aging configuration for introduced users.

Authorization: viewer

---

### Examples

The following is an example of how to display the aging of introduced users.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 user aging introduced
```

```
Introduced user aging is enabled.
```

```
Introduced user aging time is 30 minutes.
```

```
NME-APA>
```

---

### Related Commands

[user aging](#) (on page 2-255)

## show interface linecard user anonymous

Displays the users in a specified anonymous user group.

Use the “amount” form to display the number of users in the group rather than a complete listing of members.

**show interface linecard** *slot-number* **user anonymous** [**amount**] [**name** *group-name*]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*group-name* The anonymous user group.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

If no group-name is specified, all anonymous users in all groups are displayed.

Authorization: viewer

---

### Examples

The following is an example of how to display the number of users in the anonymous user group anon1.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 user anonymous amount name  
anon1
```

```
NME-APA>
```

---

### Related Commands

[clear interface linecard user](#) (on page 2-27)

## show interface linecard user anonymous-group

Displays the configuration of the specified anonymous user group.

Use the “all” form with no group name to display all existing anonymous user groups.

**show interface linecard** *slot-number* **user anonymous-group** [*name group-name*] [**all**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*group-name* The anonymous user group.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following is an example of how to display the anonymous user groups.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show interface linecard 0 user anonymous-group all
```

```
name                IP range                Template #
----                -
Group1              10.10.10.10/99         0
```

```
1 anonymous groups are configured
```

```
NME-APA>
```

---

### Related Commands

## show interface linecard user db counters

Displays the user database counters.

**show interface linecard** *slot-number* **user db counters**

---

### Syntax Description

---

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Counter Definitions

Following are definitions of the counters displayed in the output of this command.

**CURRENT VALUES:**

Users: Number of currently existing users (excluding users waiting to be removed)

Introduced/Pulled users: Number of introduced or pulled users.

Anonymous users: Number of anonymous users.

Users with mappings: Number of users with mappings.

IP mappings: Number total of IP mappings over all users including allocated ranges

VLAN Entries: Number of VLAN mappings over all users

Users with open sessions: Number of users with open flows (sessions)

Users with TIR mappings: Number of users with mapping to a TP-IP range

Sessions mapped to the default user: Number of open flows (sessions) related to the default party

**PEAK VALUES:**

Peak number of users with mappings:

Peak number occurred at:

Peak number cleared at:

**EVENT COUNTERS:**

User introduced: Number of login calls resulting in adding a user.

User pulled: Number of pullResponse calls.

User aged: Number of aged users.

Pull-request notifications sent: Number of pull request notifications sent.

Pull-request by ID notifications sent: Number of pull request notifications by ID sent.

State notifications sent: Number of state change notifications sent to peers.

Logout notifications sent: Number of logout events.

User mapping TIR contradictions: Number of contradicting configured TIRs that are invalid.

### Examples

The following example shows how to display the user database counters:

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user db counters
Current values:
=====
Users: 2 used out of 499 max.
Introduced/Pulled users: 0.
Anonymous users: 2.
Users with mappings: 0 used out of 999 max.
IP mappings: 0 used.
VLAN Entries: 0 used.
Users with open sessions: 2.
Users with TIR mappings: 0.
Sessions mapped to the default user: 0.

Peak values:
=====
Peak number of users with mappings: 5
Peak number occurred at: 00:13:50 UTC TUE August 14 2007
Peak number cleared at: 00:13:50 UTC TUE August 14 2007

Event counters:
=====
User introduced: 0.
User pulled: 0.
User aged: 0.
Pull-request notifications sent: 0.
Pull-request by ID notifications sent: 0.
User pulled by ID: 0.
State notifications sent: 0.
Logout notifications sent: 0.
User mapping TIR contradictions: 0.
NME-APA>
```

### Related Commands

[clear interface linecard user db counters](#) (on page 2-28)

## show interface linecard user mapping

Displays users whose mapping meets one of the following specified criteria:

- Is within a specified range of IP addresses
- Intersects a specified IP range
- Matches a specified VLAN tag
- Has no mapping

Use the “amount” form to display the number of users meeting the criteria rather than listing actual user names.

**show interface linecard** *slot-number* **user mapping** [**amount**] [**IP** *iprange*] [**included-in** *iprange*] [**IP** *ipaddress/range*] [**VLANid** *vlanid*] [**none**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*iprange* Specified range of IP addresses.

*vlanid* Specified VLAN tag.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

**Examples**

The following is an example that lists the number of users with no mapping.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user mapping amount none
Users with no mappings:
DefaultParty
Total 1 users listed.
NME-APA>
```

---

**Related Commands**

## show interface linecard user name

Displays information about a specified user. The following information can be displayed:

- Mappings
- OS counters (bandwidth and current number of flows)
- All values of user properties
- VAS servers used per VAS Server Group
- All of the above

If no category is specified, a complete listing of property values, mappings and counters is displayed.

**show interface linecard** *slot-number* **user name** *name* [**mappings**] [**counters**] [**properties**] [**VAS-servers**]

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*name* The user name.

*mappings* Display user mappings.

*counters* Display OS counters.

*properties* Display values of all user properties

*vas-servers* Display the VAS servers used by the specified user

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following is an example of how to list the mappings for the specified user.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user name gold123 mappings
User 'gold123' mappings:
IP 10.0.0.0 - Expiration (sec): Unlimited
NME-APA>
```

---

### Related Commands

[user name property](#) (on page 2-251)

## show interface linecard user properties

Displays all existing user properties.

**show interface linecard *slot-number* user properties**

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

---



---

### Defaults

This command has no default settings.

---

### Command Mode

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following is an example of how to display the user properties.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user properties
User properties:
"monitor" : int16, minValue=0, maxValue=1.
"new_classification_policy" : Uint16.
"packageId : Uint16, minValue=0, maxValue=4999.
"QpLimit" : int32[18].
"QpSet" : Uint8[18].
User read-only properties:
"concurrentAttacksNumber" : Uint8.
"PU_QP_QuotaSetCounter" : Uint8[18].
"PU_QP_QuotaUsageCounter" : int32[18].
"PU_REP_nonReportedSessionsInTUR" : int32.
"P_aggPeriodType" :Uint8.
"P_blockReportCounter : int32
"P_endOfAggPeriodTimestamp : Uint32.
"P_firstTimeParty" : bool.
"P_localEndOfAggPeriodTimestamp : Uint32.
"P_mibSubCounters16" : Uint16[36][2].
"P_mibSubCounters32" : Uint32[36][2].
"P_newParty" : bool.
"P_numOfRedirections : Uint8.
"P_partyCurrentPackage : Uint16
"P_partyGoOnlineTime : Uint32
"P_partyMonth : Uint16
NME-APA>
```

---

Related Commands

## show interface linecard user templates

Displays a specified user template.

**show interface linecard** *slot-number* **user templates** [**all**]**index** *template-number*

---

### Syntax Description

*slot-number* The number of the identified slot. Enter a value of 0.

*template-number* The index number of the template to be displayed.

---



---

### Defaults

This command has no default settings.

---

### Command Mode

User Exec

---

### Usage Guidelines

Use the **all** keyword to display all existing user templates.

Authorization: viewer

---

### Examples

The following is an example of how to display a specified user template.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show interface linecard 0 user templates index 3
User template 3 properties
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
NME-APA>
```

---

### Related Commands

## show inventory

Displays the following UDI information for the NME-APA module:

- Device name
- Description
- Product identifier
- Version identifier
- Serial number

### show inventory

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example displays the UDI information for the NME-APA module.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show inventory
NAME: "Chassis", DESCR: "Cisco SCE 2020 Service Control Engine,
Multi Mode, 4-port GE"
PID: SCE2020-4XGBE-MM , VID: V01, SN: CAT093604K3
NME-APA>
```

---

#### Related Commands

## show ip advertising

Shows the status of IP advertising, the configured destination and the configured interval.

Use the [destination] and [interval] versions of the command to display only the configured destination or interval, respectively.

**show ip advertising [destination|interval]**

|                    |                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <p><b>destination</b> Displays IP advertising destination.</p> <p><b>interval</b> Displays the interval between ping commands</p>                                                                                                                                                                                        |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                                                                                    |
| Command Modes      | User Exec                                                                                                                                                                                                                                                                                                                |
| Usage Guidelines   | <p>Use the form <b>show ip advertising destination</b> to display the IP advertising destination.</p> <p>Use the form <b>show ip advertising interval</b> to display the interval between ping commands.</p> <p>Authorization: viewer</p>                                                                                |
| Examples           | <p>The following example shows the IP advertising status and configuration.</p> <pre><b>NME-APA&gt;enable 5</b> <b>Password:&lt;cisco&gt;</b> <b>NME-APA&gt;show ip advertising</b> IP advertising is disabled IP advertising destination is 10.10.10.10 IP advertising interval is 853 seconds <b>NME-APA&gt;</b></pre> |
| Related Commands   | <a href="#">ip advertising</a> (on page 2-68)                                                                                                                                                                                                                                                                            |

## show ip filter

Displays the following information for management interface IP filtering.

- IP fragment filter enabled or disabled
- configured attack threshold (permitted and not-permitted IP addresses)
- configured end of attack threshold (permitted and not-permitted IP addresses)
- burst size in seconds (permitted and not-permitted IP addresses)

### show ip filter

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

**Examples**

The following command shows how to display information for management interface IP filtering

```

NME-APA>enable 5
Password:<cisco>
NME-APA> show ip filter
is fragment filtered      : 0
Input Bandwidth          : 0 Kb/sec
Input packets rate       : 2 Pkt/sec
Input bandwidth policer   : CIR: 20000.00 Kb/sec  BTime: 200
msec LP: 100 %
Input packet rate policer : CIR: 5000.00 Pkt/sec  BTime: 200
msec LP: 100 %

Permit monitor           :state : no_attack  BW: 0
High : CIR: 20000.00 Kb/sec  BTime: 10000 msec LP: 100 %
Low  : CIR: 20000.00 Kb/sec  BTime: 10000 msec LP: 100 %
Denied monitor          :state : no_attack  BW: 0
High : CIR: 20000.00 Kb/sec  BTime: 10000 msec LP: 100 %
Low  : CIR: 20000.00 Kb/sec  BTime: 10000 msec LP: 100 %
in_bytes                : 85115466
in_pkt                  : 371598
in_pkt_accept           : 371598
in_pkt_denied           : 0
drop_fragment_cnt       : 0
action_delay_due_bw     : 0
action_delay_due_pkt    : 0
  PERMIT events
    meStartAttack       : 0
    meStopAttack        : 0
  DENIED events
    meStartAttack       : 0
NME-APA>

```

**Related Commands**

[ip filter fragment](#) (on page 2-72)

[ip filter monitor](#) (on page 2-73)

## show ip radius-client

Displays the RADIUS client general configuration.

### show ip radius-client

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged Exec

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example illustrates how to use this command.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#show ip radius-client  
  
NME-APA>
```

---

**Related Commands**

[ip radius-client retry limit](#) (on page 2-79)

## show ip rpc-adapter

Displays the status of the RPC adapter (enabled or disabled) and the configured port.

**show ip rpc-adapter [sessions]**

---

**Syntax Description**

---

*sessions* Display information regarding RPC adapter sessions.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the configuration of the RPC adapter.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show ip rpc-adapter
RPC Server is ONLINE
RPC Server port is 14374
RPC Security level is full
NME-APA>
```

---

**Related Commands**

[ip rpc-adapter](#) (on page 2-80)

[ip rpc-adapter port](#) (on page 2-81)

## show line vty

Displays the Telnet configuration.

### show line vty timeout

---

#### Syntax Description

---

*timeout* Shows the timeout configured to the Telnet sessions.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the timeout duration.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show line vty timeout  
Timeout is 30 minutes  
NME-APA>
```

---

#### Related Commands

[line vty](#) (on page 2-83)

## show log

Displays the contents of the user log file.

### show log

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example illustrates the use of this command.

```

NME-APA>enable 5
Password:<cisco>
NME-APA>show log
2006-01-25 00:14:46 | INFO | CPU #000 | User message files
were successfully cleared, new files were opened
2006-01-25 00:23:07 | INFO | CPU #000 | A new password was set
for level 10
2006-01-25 00:49:41 | INFO | CPU #000 | System hostname
changed to :ecco"
2006-01-25 01:02:41 | INFO | CPU #000 | Time zone set to GMT
2006-01-25 01:06:33 | INFO | CPU #000 | A new password was set
for level 15
2006-01-25 01:08:07 | INFO | CPU #000 | A new password was set
for level 5
2006-01-25 01:23:07 | INFO | CPU #000 | IP address of slot 0,
port 0 set to 10.10.10
2006-01-25 01:56:44 | INFO | CPU #000 | Configuration file
'/tffs0/system/config.txt' was saved - file size 1200
2006-01-25 05:34:45 | INFO | CPU #000 | A telnet session from
20.20.20.20 was established
NME-APA>

```

---

**Related Commands**

[clear logger](#) (on page 2-29)

[logger get user-log file-name](#) (on page 2-90)

[more user-log](#) (on page 2-98)

## show logger device

Displays the configuration of the specified NME-APA module logger file.

Also displays the current user log counters.

**show logger device {line-attack-file-log | user-file-log[counters|max-file-size|status|nv-counters]}**

---

### Syntax Description

See "Usage Guidelines".

---



---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Specify the desired logger device:

- **Line-Attack-File-Log:** displays the following information:
  - Status
  - Maximum file size
- **SCE-agent-Statistics-Log:** displays the following information:
  - Status
  - Maximum file size
  - Maximum number of backup files
- **User-File-Log:** displays the following information:
  - Status
  - Maximum file size

If you specify **User-File-Log**, you can specify one of the following options:

- **counters:** Displays the User-File-Log counters
- **max-file-size:** Displays the currently configured maximum file size for the User-File-Log
- **nv-counters:** Displays the User-File-Log non-volatile counters
- **status:** Displays the current status of the User-File-Log

Authorization: viewer

**Examples**

The following examples illustrate the use of this command.

**EXAMPLE 1**

The following example shows the NME-APA module Line-Attack-File-Log status and configuration.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show logger device line-attack-file-log
Line-Attack-File-Log status: Enabled
Line-Attack-File-Log file size: 1000000
NME-APA>
```

**EXAMPLE 2**

The following example shows the NME-APA module SCE-agent-Statistics-Log status and configuration.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show logger device sce-agent-statistics-log
Device SCE-agent-Statistics-Log status: Enabled
Device SCE-agent-Statistics-Log max file size: 204800
Device SCE-agent-Statistics-Log max backup files: 10
NME-APA>
```

**EXAMPLE 3**

The following example shows the NME-APA module User-File-Log counters.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show logger device line-attack-file-log counters
Logger device User-File-Log counters
Total info messages:      62
Total warning messages:   4
Total error messages:     0
Total fatal messages:     0
Last time these counters were cleared: 02:23:27 GMT TUES
January 17 2006
NME-APA>
```

**Related Commands**

[logger device](#) (on page 2-87)

[clear logger](#) (on page 2-29)

## show pqi file

Displays information, such as installation options, about the specified application file.

**show pqi file *filename* info**

---

### Syntax Description

---

*filename* The filename of the desired application file.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

User Exec

---

### Usage Guidelines

Authorization: viewer

---

### Examples

The following example shows how to display application file information.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show pqi file stf30519.pqi info
application:    SCAS BB
version:       3.0.5 build 19
description:    Installs SCAS BB on NME-APA
```

```
Available installation options:
'capacityOption=StarfleetDefaultNME-APA '
'capacityOption=SubscriberLessNME-APA '
```

```
target device: SENME-APA
module names:  stf30519.pm0
NME-APA>
```

---

### Related Commands

[pqi install file](#) (on page 2-103)

## show pqi last-installed

Displays the name of the last pqi file that was installed.

### show pqi last-installed

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows how to find out what pqi file is installed.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show pqi last-installed
package name:    SCAS BB
package version 3.0.5 build 19
package date:    Mon Aug 13 17:27:55 GMT+00:00 2007
operation:       Install
NME-APA>
```

---

**Related Commands**

[pqi rollback file](#) (on page 2-104)

[pqi uninstall file](#) (on page 2-105)

## show rdr-formatter

Displays the RDR formatter configuration.

### show rdr-formatter

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the configuration of the RDR formatter.

```

NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter
Status: enabled
Connection is: down
Forwarding mode: multicast
no destination is set for the RDR Formatter
RDR:   queued:      7 ,sent:      0, thrown:      0
UM:    queued:      0 ,sent:      0, thrown:      0
Logger: queued:      0 ,sent:      0, thrown:      0
Errors: thrown:      0
Last time these counters were cleared: 17:41:26 UTC WED August 8
2007
NME-APA>

```

---

**Related Commands**

[rdr-formatter destination](#) (on page 2-110)

[service rdr-formatter](#) (on page 2-124)

## show rdr-formatter connection-status

Shows the current RDR formatter connection table and status (main connection status: up/down, forwarding mode, and connection/activity information for each destination).

### show rdr-formatter connection-status

#### Syntax Description

This command has no arguments or keywords.

#### Defaults

This command has no default settings.

#### Command Modes

User Exec

#### Usage Guidelines

Authorization: viewer

#### Examples

The following example shows the RDR-formatter connection status.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter connection-status
Connection is: down
Forwarding mode: redundancy
no destination is set for the RDR Formatter
NME-APA>
```

#### Related Commands

[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter counters](#) (on page 2-183)  
[show rdr-formatter destination](#) (on page 2-184)  
[show rdr-formatter enabled](#) (on page 2-185)  
[show rdr-formatter forwarding-mode](#) (on page 2-186)  
[show rdr-formatter history-size](#) (on page 2-187)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)  
[show rdr-formatter statistics](#) (on page 2-190)

## show rdr-formatter counters

Shows the RDR-formatter counters.

### show rdr-formatter counters

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the RDR-formatter counters.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter counters
RDR:   read:      0 ,sent:      0, thrown:      0
UM:    read:      0 ,sent:      0, thrown:      0
Logger: read:      0 ,sent:      0, thrown:      0
Errors: thrown:      0
Last time these counters were cleared: 14:05:57 GMT SUN January
23 2006
NME-APA>
```

---

#### Related Commands

[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter connection-status](#) (on page 2-182)  
[show rdr-formatter destination](#) (on page 2-184)  
[show rdr-formatter enabled](#) (on page 2-185)  
[show rdr-formatter forwarding-mode](#) (on page 2-186)  
[show rdr-formatter history-size](#) (on page 2-187)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)  
[show rdr-formatter statistics](#) (on page 2-190)

## show rdr-formatter destination

Shows the RDR-formatter destinations.

### show rdr-formatter destination

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the RDR-formatter configured destinations.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter destination
Destination: 10.1.1.205
Port: 33000
Destination: 10.1.1.206
Port: 33000
Destination: 10.10.12.10
Port: 33000
NME-APA>
```

---

#### Related Commands

[rdr-formatter destination](#) (on page 2-110)  
[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter connection-status](#) (on page 2-182)  
[show rdr-formatter counters](#) (on page 2-183)  
[show rdr-formatter enabled](#) (on page 2-185)  
[show rdr-formatter forwarding-mode](#) (on page 2-186)  
[show rdr-formatter history-size](#) (on page 2-187)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)  
[show rdr-formatter statistics](#) (on page 2-190)

## show rdr-formatter enabled

Shows the RDR-formatter status (enabled/disabled).

### show rdr-formatter enabled

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows that the RDR formatter is enabled.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter enabled
Status:  enabled
NME-APA>
```

---

**Related Commands**

[service rdr-formatter](#) (on page 2-124)  
[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter connection-status](#) (on page 2-182)  
[show rdr-formatter counters](#) (on page 2-183)  
[show rdr-formatter destination](#) (on page 2-184)  
[show rdr-formatter forwarding-mode](#) (on page 2-186)  
[show rdr-formatter history-size](#) (on page 2-187)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)  
[show rdr-formatter statistics](#) (on page 2-190)

## show rdr-formatter forwarding-mode

Shows the configured RDR-formatter forwarding-mode (redundancy/multicast/simple load balancing).

### show rdr-formatter forwarding-mode

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the RDR formatter forwarding-mode.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter forwarding-mode
Forwarding mode:  redundancy
NME-APA>
```

---

#### Related Commands

[rdr-formatter forwarding-mode](#) (on page 2-112)  
[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter connection-status](#) (on page 2-182)  
[show rdr-formatter counters](#) (on page 2-183)  
[show rdr-formatter destination](#) (on page 2-184)  
[show rdr-formatter enabled](#) (on page 2-185)  
[show rdr-formatter history-size](#) (on page 2-187)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)  
[show rdr-formatter statistics](#) (on page 2-190)

## show rdr-formatter history-size

Shows the configured size of the RDR formatter history buffer.

### show rdr-formatter history-size

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the size of the RDR formatter history buffer.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show rdr-formatter history-size  
History buffer size: 16000 bytes  
NME-APA>
```

---

**Related Commands**

[rdr-formatter history-size](#) (on page 2-113)  
[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter connection-status](#) (on page 2-182)  
[show rdr-formatter counters](#) (on page 2-183)  
[show rdr-formatter destination](#) (on page 2-184)  
[show rdr-formatter enabled](#) (on page 2-185)  
[show rdr-formatter forwarding-mode](#) (on page 2-186)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)  
[show rdr-formatter statistics](#) (on page 2-190)

## show rdr-formatter rdr-mapping

Shows to which RDR formatter category a specified RDR tag is mapped.

**show rdr-formatter rdr-mapping all***|tag-ID*

---

**Syntax Description**

*tag-ID* The RDR tag to be displayed (in HEX).

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Use the **all** keyword to display all current RDR-category mappings.

Authorization: viewer

---

**Examples**

The following example illustrates the use of this command, showing partial output:

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter rdr-mapping all
Tag                Categories
---                -
0xb2d05e01        1
0xb2d05e02        1
0xb2d05e04        1
0xb2d05e05        1
0xf0f0f000        1
0xf0f0f002        1
0xf0f0f004        1
0xf0f0f005        1
0xf0f0f010        1
0xf0f0f016        1
0xf0f0f017        1
0xf0f0f018        1
---More---
```

**NME-APA>**

---

**Related Commands**

[rdr-formatter rdr-mapping](#) (on page 2-114)

[show rdr-formatter](#) (on page 2-181)

[show rdr-formatter connection-status](#) (on page 2-182)

[show rdr-formatter counters](#) (on page 2-183)

*show rdr-formatter destination* (on page 2-184)

*show rdr-formatter enabled* (on page 2-185)

*show rdr-formatter forwarding-mode* (on page 2-186)

*show rdr-formatter history-size* (on page 2-187)

*show rdr-formatter statistics* (on page 2-190)

## show rdr-formatter statistics

Shows the current RDR formatter statistics.

### show rdr-formatter statistics

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the current RDR statistics.

```

NME-APA>enable 5
Password:<cisco>
NME-APA>show rdr-formatter statistics
RDR-formatter statistics
=====
Category 1
  sent:      0
  in-queue:  0
  thrown:    0
  rate:      0 RDRs per second
  max rate:  0 RDRs per second

Category 2
  sent:      0
  in-queue:  0
  thrown:    0
  rate:      0 RDRs per second
  max rate:  0 RDRs per second

```

```
Category 3
  sent:      0
  in-queue:  0
  thrown:    0
  rate:      0 RDRs per second
  max rate:  0 RDRs per second

Category 4
  sent:      0
  in-queue:  0
  thrown:    0
  rate:      0 RDRs per second
  max rate:  0 RDRs per second
Destination: 10.1.1.205 Port: 33000 Status: down
  Sent:      0
  Rate: 0    Max: 0
Last connection establishment: 2 days, 10 hours, 25 minutes,
40 seconds
Destination: 10.1.1.206 Port: 33000 Status: down
  Sent:      0
  Rate: 0    Max: 0
Last connection establishment: 13 hours, 32 minutes, 58 seconds
Destination: 10.10.12.10 Port: 33000 Status: down
  Sent:      0
  Rate: 0    Max: 0
Last connection establishment: 2 days, 8 hours, 34 minutes, 14
seconds
NME-APA>
```

---

**Related Commands**

[show rdr-formatter](#) (on page 2-181)  
[show rdr-formatter connection-status](#) (on page 2-182)  
[show rdr-formatter counters](#) (on page 2-183)  
[show rdr-formatter destination](#) (on page 2-184)  
[show rdr-formatter enabled](#) (on page 2-185)  
[show rdr-formatter forwarding-mode](#) (on page 2-186)  
[show rdr-formatter history-size](#) (on page 2-187)  
[show rdr-formatter rdr-mapping](#) (on page 2-188)

## show running-config

Shows the current configuration.

**show running-config [all-data]**

---

**Syntax Description**

---

**all data** Displays defaults as well as non-default settings.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

Use the **all data** switch to see sample usage for many CLI configuration commands.

Authorization: admin

---

**Examples**

The following example shows the partial output of the **show running-config** command.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#>show running-config all-data
#This is a general configuration file (running-config).
#Created on 16:48:11 UTC WED May 13 2006

cli-type 1
#version 1

service logger

no service password-encryption
enable password level 10 0 "cisco"
enable password level 15 0 "cisco"
service RDR-formatter
no RDR-formatter destination all
RDR-formatter history-size 0
clock timezone UTC 0
ip domain-lookup
no ip domain-name
no ip name-server
service telnetd
```

```
FastEthernet 0/0
ip address 10.1.5.120 255.255.0.0
speed auto
duplex auto
```

```
exit
ip default-gateway 10.1.1.1
no ip route all
```

```
line vty 0 4
no access-class in
timeout 30
exit
NME-APA#
```

---

**Related Commands**

*more* (on page [2-96](#))

## show snmp

Displays the SNMP configuration and counters.

### **show snmp**

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Counter Definitions**

Following are definitions of the counters displayed in the output of this command.

SNMP packets input - Total number of messages delivered to the SNMP entity from the transport service.

Bad SNMP version errors - Total number of SNMP messages delivered to the SNMP protocol entity that were for an unsupported SNMP version.

Unknown community name - Total number of SNMP messages delivered to the SNMP protocol entity that used a SNMP community name not known to said entity.

Illegal operation for community name supplied - Total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation not allowed by the SNMP community named in the message.

Encoding errors - Total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.

Number of requested variables - Total number of MIB objects successfully retrieved by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

Number of altered variables - Total number of MIB objects that have been successfully altered by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

Get-request PDUs - Total number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.

Get-next PDUs - Total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.

Set-request PDUs - Total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.

SNMP packets output - Total number of SNMP Messages passed from the SNMP protocol entity to the transport service.

Too big errors - Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is `tooBig'.

No such name errors - Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status is `noSuchName'.

Bad values errors - Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is `badValue'.

General errors - Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is `genErr'.

Response PDUs - Total number of SNMP Get-Response PDUs generated by the SNMP protocol entity.

Trap PDUs - Total number of SNMP Trap PDUs generated by the SNMP protocol entity.

### Examples

The following example shows the SNMP server configuration and statistics.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show snmp
SNMP Agent is enabled
Location has no text
Contact has no text
Authentication-failure trap status: Disabled
operational-status traps status:      Enabled
system-reset trap status:             Enabled
chassis traps status:                 Enabled
RDR-formatter traps status:           Disabled
Telnet traps status:                  Enabled
logger traps status:                  Enabled
SNTP traps status:                   Enabled
link-bypass traps status:             Disabled
user traps status:                    Disabled
pull-request-failure traps status:    Disabled
attack traps status:                  Disabled
vas-traffic-forwarding traps status:  Disabled
port-operational-status traps status: Disabled
mpls-vpn traps status:                Disabled
```

```

Communities:
-----
Community: Public,          Access Authorization: RO,          Access
List Index: 0
Trap managers:
-----
Trap host: 171.71.9.246,          community: abc,
version: SNMPv2c
snmpInPkts.0=310
snmpOutPkts.0=349
snmpInBadVersions.0=0
snmpInBadCommunityNames.0=3
snmpInBadCommunityUses.0=0
snmpInASNParseErrs.0=0
snmpInTooBigs.0=0
snmpInNoSuchNames.0=0
snmpInBadValues.0=0
snmpInReadOnlys.0=0
snmpInGenErrs.0=0
snmpInTotalReqVars.0=1377
snmpInTotalSetVars.0=0
snmpInGetRequests.0=0
snmpInGetNexts.0=306
snmpInSetRequests.0=0
snmpInGetResponses.0=0
snmpInTraps.0=0
snmpOutTooBigs.0=0
snmpOutNoSuchNames.0=0
snmpOutBadValues.0=0
snmpOutGenErrs.0=0
snmpOutGetRequests.0=0
snmpOutGetNexts.0=0
snmpOutSetRequests.0=0
snmpOutGetResponses.0=306
snmpOutTraps.0=43
snmpEnableAuthenTraps.0=disabled(2)
snmpSilentDrops.0=0
snmpProxyDrops.0=0
NME-APA>

```

---

**Related Commands**

*show snmp community* (on page 2-198)

*show snmp contact* (on page 2-199)

*show snmp enabled* (on page 2-200)

*show snmp host* (on page 2-201)

*show snmp location* (on page 2-202)

## show snmp community

Displays configured communities.

### **show snmp community**

---

#### Syntax Description

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the SNMP manager communities.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show snmp community
Community: public, Access Authorization: RO,
Access List Index: 1
NME-APA>
```

---

#### Related Commands

[snmp-server community](#) (on page 2-223)  
[show snmp](#) (on page 2-194)

## show snmp contact

Displays the configured MIB-2 variable sysContact.

### show snmp contact

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the system contact.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show snmp contact  
Contact: Brenda@mycompany.com  
NME-APA>
```

---

#### Related Commands

[snmp-server contact](#) (on page 2-224)

[show snmp](#) (on page 2-194)

## show snmp enabled

Displays the SNMP agent status (enabled/disabled).

### show snmp enabled

---

#### Syntax Description

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the SNMP server enabled status.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show snmp enabled
SNMP Agent is enabled
NME-APA>
```

---

#### Related Commands

[snmp-server](#) (on page 2-222)

[show snmp](#) (on page 2-194)

## show snmp host

Displays the destination hosts for SNMP traps.

### show snmp host

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the destination hosts for SNMP traps.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show snmp host
```

```
Trap host: 10.1.1.205, community: public, version: SNMPv2c
```

```
NME-APA>
```

---

#### Related Commands

[snmp-server host](#) (on page 2-227)

[show snmp](#) (on page 2-194)

## show snmp location

Displays the configured MIB-2 variable sysLocation.

### show snmp location

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the system location.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show snmp location
Location: London_Office
NME-APA>
```

---

#### Related Commands

[snmp-server location](#) (on page 2-228)

[show snmp](#) (on page 2-194)

## show snmp mib

Displays MIB variables.

**show snmp mib** *mib variables*

| Syntax Description |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <p><i>mib</i> Name of MIB to display.</p> <p><b>MIB-II</b></p> <p><b>cisco-copy-config</b></p> <p><b>cisco-queue</b></p> <p><b>cisco-service-control-attack</b></p> <p><b>cisco-service-control-controller</b></p> <p><b>cisco-service-control-link</b></p> <p><b>cisco-service-control-rdr</b></p> <p><b>cisco-service-control-user</b></p> <p><b>cisco-service-control-tp-stats</b></p> <p><b>cisco-syslog-event-ext</b></p> <p><b>entity</b></p> <p><b>entity-state</b></p> <p><b>host-resource</b></p> |
|                    | <p><i>variables</i> Name of group to display.</p> <p><b>MIB-II:</b> Use one of the following values: AT, ICMP, interfaces, IP, SNMP, system, TCP or UDP.</p>                                                                                                                                                                                                                                                                                                                                               |
| Defaults           | This command has no default settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Command Modes      | User Exec                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Usage Guidelines   | Authorization: viewer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

---

**Examples**

The following example shows the MIB-2 system group.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show snmp mib MIB-II system
sysDescr.0 = Cisco Service Engineering,
SW version: Control Card Version 1.30 build 29,
HW version: NME-APA GE "RevE"
sysObjectID.0 = 1.3.6.1.4.1.5655.1.2
sysUpTime.0 = 14 hours, 25 minutes, 59 seconds
sysContact.0 = Brenda@mycompany.com
sysName.0 = NME-APA
sysLocation.0 = London_Office
sysServices.0 = 2
NME-APA>
```

---

**Related Commands**

## show snmp traps

Displays the SNMP traps generation status (enabled/disabled).

### show snmp traps

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the SNMP server traps status.

```

NME-APA>enable 5
Password:<cisco>
NME-APA>show snmp traps
Authentication-failure trap status: Disabled
operational-status traps status:   Enabled
system-reset trap status:          Enabled
chassis traps status:              Enabled
RDR-formatter traps status:        Disabled
Telnet traps status:               Enabled
logger traps status:               Enabled
SNTP traps status:                 Enabled
link-bypass traps status:          Disabled
user traps status:                 Disabled
pull-request-failure traps status: Disabled
attack traps status:               Disabled
vas-traffic-forwarding traps status: Disabled
port-operational-status traps status: Disabled
mpls-vpn traps status:             Disabled
NME-APA>

```

---

**Related Commands**

[snmp-server enable traps](#) (on page 2-225)

## show sntp

Displays the SNTP configuration and update statistics.

### show sntp

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows statistics from the SNTP clients.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show sntp
SNTP broadcast client: disabled
last update time: not available

SNTP uni-cast client: enabled
there is one server:
1: 128.182.58.100
last update time: Feb 10 2002, 14:06:41
update interval: 100 seconds
```

```
NME-APA>
```

---

**Related Commands**

[sntp server](#) (on page 2-230)  
[sntp broadcast client](#) (on page 2-229)  
[sntp update-interval](#) (on page 2-231)

## show startup-config

Shows the startup configuration file. Use this command to review the configuration used by the NME-APA module at boot time in comparison with the current configuration to make sure that you approve of all the differences before saving the configuration by using **copy running-config startup-config** command.

### show startup-config

---

#### Syntax Description

---

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privileged EXEC

---

#### Usage Guidelines

Authorization: admin

---

#### Examples

The following example shows a sample output.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#show startup-config
#Created on 20:17:46 UTC THU January 1 2001
#cli-type 1
#version 1
logger NME-APA User-File-Log max-file-size 20000
ip domain-name *<cisco>*
ip name-server 10.1.1.1
interface FastEthernet 0/0
ip address 10.1.4.202 255.0.0.0
interface linecard 0
silent
NME-APA#
```

---

#### Related Commands

[more](#) (on page 2-96)

## show system operation-status

Displays the operation status of the system.

### show system operation-status

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the system operation status:

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show system operation-status
System Operation status is Operational
Port status is:
Link on port #1 is down
Link on port #2 is down
NME-APA>
```

---

#### Related Commands

## show system-uptime

Displays the length of time the system has been running since the last reboot..

### show system-uptime

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the system uptime for the NME-APA module.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show system-uptime
```

```
NME-APA uptime is 4 days, 13 hours, 21 minutes, 37 seconds
```

```
NME-APA>
```

---

#### Related Commands

## show tacacs

Displays statistics for the TACACS+ servers.

### show tacacs

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

The **'all'** option is available only at the Privileged Exec level.

Use the **all** keyword to display keys and timeouts as well as other statistics.

---

#### Usage Guidelines

Note that, although most show commands are accessible to viewer level users, the **'all'** option is available only at the admin level. Use the command **'enable 10'** to access the admin level.

Authorization: viewer

The **'all'** option is at the admin authorization level.

---

#### Examples

The following examples illustrate how to use this command.

##### EXAMPLE 1

This example shows how to display statistics for all TACACS+ servers.

```
NME-APA>enable 5
Password:<cisco>
NME-APA> show tacacs
Server: 100.10.10.10./49: opens=0 closes=0 error=0
      messages in=0 messages out=0
NME-APA>
```

##### EXAMPLE 2

This example shows how to display statistics, including keys and timeouts, for all TACACS+ servers.

```
NME-APA>enable 10
Password:<cisco>
NME-APA# show tacacs all
Server: 100.10.10.10./49: opens=0 closes=0 error=0
      messages in=0 messages out=0
      timeout=20
      uses default timeout= yes
      key= a
      uses default key= no
NME-APA#
```

---

**Related Commands**

[tacacs-server host](#) (on page 2-232)

[tacacs-server key](#) (on page 2-234)

[tacacs-server timeout](#) (on page 2-235)

## show telnet sessions

Displays any active Telnet sessions.

### show telnet sessions

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows that there is one active Telnet session.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show telnet sessions
There is 1 active telnet session:

Index | Source
=====
  0   | 10.1.1.201
NME-APA>
```

---

#### Related Commands

[telnet](#) (on page 2-236)

[show telnet status](#) (on page 2-213)

## show telnet status

Displays the status of the telnet server daemon.

### show telnet status

---

**Syntax Description**

---

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows that the telnet daemon is currently enabled.

```
NME-APA>enable 5  
Password:<cisco>  
NME-APA>show telnet status  
Telnet daemon is enabled.  
NME-APA>
```

---

**Related Commands**

[service telnetd](#) (on page 2-125)

[show telnet sessions](#) (on page 2-212)

## show timezone

Displays the current time zone and daylight saving time configuration as configured by the user.

### show timezone

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the time zone configured by the user.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show timezone
```

```
Time zone: ISR    minutes offset from UTC: 120
```

```
NME-APA>
```

---

**Related Commands**

[clock timezone](#) (on page 2-39)

## show users

Displays the users in the local database, including passwords.

### show users

---

#### Syntax Description

---

This command has no arguments or keywords.

---

---

#### Defaults

This command has no default settings.

---

#### Command Modes

Privilege Exec

---

#### Usage Guidelines

Note that, although most show commands are accessible to viewer level users, this command is available only at the admin level. Use the command **'enable 10'** to access the admin level.

Authorization: admin

---

#### Examples

This example shows how to display the users in the local database.

```
NME-APA>enable 10
Password:<cisco>
NME-APA# show users
User:  name = Joe
       privilege level = 10
       password = joespwd
       is password encrypted = no
NME-APA#
```

---

#### Related Commands

[username](#) (on page 2-256)

## show version

Displays the configuration information for the system including the hardware version, the software version, the application used, and other configuration information.

### show version

---

**Syntax Description**


---

This command has no arguments or keywords.

---



---

**Defaults**

This command has no default settings.

---

**Command Modes**

User Exec

---

**Usage Guidelines**

Authorization: viewer

---

**Examples**

The following example shows the current version information of the NME-APA module.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show version
NME-APA version: 0.1.4.8
SCOS version: Version 3.1.0 Build 32 - Branch: TH
  Build time: Aug  4 2007, 02:47:08

Module Type: NME-APA - 2xFE
Module S/N:   FOC10222NMQ
Chassis Type: C3845
Chassis S/N:  FHK0831F06N

SML Application information is:
Application file: /root/tffs0/app/NME-
APA_Starfleet00025_debug.sli
Application name: Starfleet SML Version 0.0.0 build 06 Debug
Version
  Using Lib - PL_Starfleet_1.0.0
  Using Lib - Classifier_StarfleetB1.0.0
Application help: Entry point of Starfleet
Original source file:
/auto/wshongrliu/work/App/SML/Engage/Starfleet/v1.0.0/dev/src/co
m/pcube/apptemplate/mn
Compilation date: Wed, August 08, 2007 at 19:10:39
Compiler version: SANc v3.05 Build 16 gcc_codelets=true built
on: Tue 03/01/2007 09:59:46.;SME plugin v1.1
Default capacity option used.
```

```
Logger status: Enabled
```

```
Management agent interface version: SCE Agent 3.1.0 Build 177
```

```
NME-APA uptime is 22 hours, 49 minutes, 6 seconds
```

```
NME-APA>
```

---

**Related Commands**

[show version all](#) (on page 2-218)

[show version software](#) (on page 2-220)

## show version all

Displays the complete version information as well as the running configuration for all components.

### show version all

#### Syntax Description

This command has no arguments or keywords.

#### Defaults

This command has no default settings.

#### Command Modes

User Exec

#### Usage Guidelines

Authorization: viewer

#### Examples

The following example shows version and configuration information for all the system components.

```
NME-APA>enable 5
```

```
Password:<cisco>
```

```
NME-APA>show version all
```

```
NME-APA version: 0.1.4.8
```

```
SCOS version: Version 3.1.0 Build 32 - Branch: TH
```

```
Build time: Aug 4 2007, 02:47:08
```

```
Module Type: NME-APA - 2xFE
```

```
Module S/N: FOC10222NMQ
```

```
Chassis Type: C3845
```

```
Chassis S/N: FHK0831F06N
```

```
SML Application information is:
```

```
Application file: /root/tffs0/app/NME-
```

```
APA_Starfleet00025_debug.sli
```

```
Application name: Starfleet SML Version 0.0.0 build 06 Debug  
Version
```

```
Using Lib - PL_Starfleet_1.0.0
```

```
Using Lib - Classifier_StarfleetB1.0.0
```

```
Application help: Entry point of Starfleet
```

```
Original source file:
```

```
/auto/wshongrliu/work/App/SML/Engage/Starfleet/v1.0.0/dev/src/co  
m/pcube/apptemplate/mn
```

```
Compilation date: Wed, August 08, 2007 at 19:10:39
```

```
Compiler version: SANc v3.05 Build 16 gcc_codelets=true built  
on: Tue 03/01/2007 09:59:46.;SME plugin v1.1
```

```
Default capacity option used.
```

```
Logger status: Enabled
```

```
Management agent interface version: SCE Agent 3.1.0 Build 177
```

```
Current configuration:
```

```
=====
```

```
#This is a general configuration file (running-config).
```

```
#Created on 16:34:38 UTC THU August 9 2007
```

```
.
```

```
.
```

```
ip rpc-adapter security-level full
```

```
ip ftp-server
```

```
NME-APA uptime is 22 hours, 53 minutes, 52 seconds
```

```
NME-APA>
```

---

**Related Commands**

[show version](#) (on page 2-216)

[show version software](#) (on page 2-220)

## show version software

Displays version information for the current software.

### show version software

---

#### Syntax Description

This command has no arguments or keywords.

---



---

#### Defaults

This command has no default settings.

---

#### Command Modes

User Exec

---

#### Usage Guidelines

Authorization: viewer

---

#### Examples

The following example shows the current software version.

```
NME-APA>enable 5
Password:<cisco>
NME-APA>show version software
Software version is: Version 3.1.0 Build 32 - Branch: TH
NME-APA>
```

---

#### Related Commands

[show version](#) (on page 2-216)

[show version all](#) (on page 2-218)

## silent

Disables the linecard from reporting events. Use the [no] form of this command if you want the linecard to send reports.

**silent**

**no silent**

---

### Syntax Description

This command has no arguments or keywords.

---

---

### Defaults

No silent

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example changes the linecard state to silent.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#silent
NME-APA(config if)#
```

---

### Related Commands

[show interface linecard silent](#) (on page 2-152)

## snmp-server

Enables the SNMP agent. You can use any of the other SNMP-server commands to enable the SNMP agent.

Use the **no** form to disable the SNMP agent from responding to SNMP managers. All SNMP settings are saved and are restored when the SNMP agent is re-enabled.

**snmp-server enable**

**no snmp-server**

|                    |                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | This command has no arguments or keywords                                                                                                                                                                       |
| Defaults           | disabled                                                                                                                                                                                                        |
| Command Modes      | Global Configuration                                                                                                                                                                                            |
| Usage Guidelines   | <p>You must define at least one community string in order to allow SNMP access. For complete information on community strings.</p> <p>Authorization: admin</p>                                                  |
| Examples           | <p>The following example disables the SNMP server.</p> <pre><b>NME-APA&gt;</b>enable 10 Password:&lt;cisco&gt; <b>NME-APA#</b>config <b>NME-APA</b>(config)#<b>no snmp-server</b> <b>NME-APA</b>(config)#</pre> |
| Related Commands   | <p><a href="#">snmp-server community</a> (on page 2-223)</p> <p><a href="#">show snmp</a> (on page 2-194)</p>                                                                                                   |

## snmp-server community

Sets a community string. Use the **no** form of the command to remove a community string.

**snmp-server community** *community-string* [*read-option*]

**no snmp-server community** *community-string* [*read-option*]

**no snmp-server community all**

---

### Syntax Description

*community-string* The SNMPv1 and SNMPv2c security string that identifies a community of managers that can access the SNMP server.

*read-option* Legal values are **ro** and **rw**. The default **ro** (read-only) option allows managers to view MIB variables. **rw** sets the variable to read-write.

---



---

### Defaults

no SNMP access

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Use the **all** keyword with the **no** form of the command to remove all configured communities.

Authorization: admin

---

### Examples

The following example configures an SNMP managers community that has read-only permissions for the NME-APA module MIB. Only SNMP managers in access list 1 can access the NME-APA module.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#snmp-server community public ro 1
NME-APA(config)#
```

---

### Related Commands

## snmp-server contact

Sets the MIB-2 variable sysContact. Use the **no** form of this command to remove the contact setting.

**snmp-server contact** *contact*

**no snmp-server contact**

|                    |                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>contact</i> A string that identifies the system contact.                                                                                                                                                                                      |
| Defaults           | This command has no default settings.                                                                                                                                                                                                            |
| Command Modes      | Global Configuration                                                                                                                                                                                                                             |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                             |
| Examples           | <p>The following example configures the system contact.</p> <pre> <b>NME-APA</b>&gt;enable 10 Password:&lt;cisco&gt; <b>NME-APA</b>#config <b>NME-APA</b>(config)#<b>snmp-server contact</b> Brenda@MyCompany.com <b>NME-APA</b>(config)# </pre> |
| Related Commands   | <a href="#">show snmp contact</a> (on page 2-199)                                                                                                                                                                                                |

## snmp-server enable traps

Enables/disables SNMP traps (only authentication-failure traps and enterprise traps can be controlled using this command). Use the **[default]** form of this command to reset SNMP traps to the default status.

**snmp-server enable traps [snmp [*snmp trap name*] ] [enterprise [*enterprise trap name*] ]**

**no snmp-server enable traps [snmp [*snmp trap name*] ] [enterprise [*enterprise trap name*] ]**

**default snmp-server enable traps [snmp [*snmp trap name*] ] [enterprise [*enterprise trap name*] ]**

---

### Syntax Description

*snmp trap name* Optional parameter used with the **snmp** parameter to control a specific snmp trap.

Setting = **Authentication**

*enterprise trap name* Optional parameter used with the **enterprise** parameter to control a specific enterprise trap.

Settings = **attack, chassis, link-bypass, logger, operational-status, port-operational-status, pull-request-failure, RDR-formatter, session, SNMP, system-reset, telnet, user, vas-traffic-forwarding**

---



---

### Defaults

snmp traps: disabled

enterprise traps: enabled

---

### Command Modes

Global Configuration

---

### Usage Guidelines

There are two classes of SNMP traps that are controlled by this command

- snmp traps
- enterprise traps

The options **snmp** and **enterprise** are parameters specifying the class of traps that are to be enabled/disabled by this command. Each class, or type, is composed of specific traps. Use these parameters as follows:

- To enable/disable all traps of one type: Specify only **snmp** or **enterprise**.
- To enable/disable only one specific trap: Specify **snmp** or **enterprise** with the additional trap name parameter naming the desired trap.
- To enable/disable all traps: Do not specify either **snmp** or **enterprise**.

Since, at this time, the only snmp type trap is the authentication trap, the **snmp** and **authentication** parameters are currently redundant.

Authorization: admin

The following example configures the SNMP server to send traps.

---

**Examples**

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#config  
NME-APA(config)#snmp-server enable traps  
NME-APA(config)#
```

---

**Related Commands**

[show snmp traps](#) (on page 2-205)

## snmp-server host

Sets destination hosts for SNMP traps.

**snmp-server host** *address* [**traps**] [**version** *version*] *community-string*

**no snmp-server host** *address* [**traps**] [**version** *version*] *community-string*

**no snmp-server host all**

### Syntax Description

|                         |                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <i>address</i>          | The IP address of the SNMP server host.                                                                                 |
| <b>traps</b>            | Optional switch, does not influence command functionality.                                                              |
| <i>version</i>          | Version of the NME-APA module software running in the system. Can be set to 1 or 2c.                                    |
| <i>community-string</i> | The SNMPv1 and SNMPv2c security string that identifies a community of managers that are able to access the SNMP server. |

### Defaults

No hosts

### Command Modes

Global Configuration

### Usage Guidelines

If no communities are specified by the **snmp-server community** command, the community string specified by this command is used by the NME-APA module, as if an **snmp-server community community-string ro** was given.

Use the **all** keyword with the **no** form of the command to remove all configured hosts.

Authorization: admin

### Examples

The following example adds a host destination for SNMP traps.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#snmp-server host 10.1.1.205 version 2c public
NME-APA(config)#
```

### Related Commands

[show snmp host](#) (on page 2-201)

## snmp-server location

Gives a name to the NME-APA module location, setting the MIB-2 variable sysLocation. Use the **no** form of this command to remove the location setting.

**snmp-server location** *location*

**no snmp-server location**

|                    |                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>location</i> A string that specifies the system location.                                                                                                                                                                                          |
| Defaults           | no location                                                                                                                                                                                                                                           |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                  |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                  |
| Examples           | <p>The following example configures the system location.</p> <pre> <b>NME-APA</b>&gt;enable 10 Password:&lt;cisco&gt; <b>NME-APA</b>#config <b>NME-APA</b>(config)#<b>snmp-server location</b> London_Office <b>NME-APA</b>(config)#           </pre> |
| Related Commands   | <a href="#">show snmp location</a> (on page 2-202)                                                                                                                                                                                                    |

## sntp broadcast client

Enables the SNTP multicast client to accept SNTP broadcasts from any SNTP server.

Use the **no** form of this command to disable the SNTP multicast client.

**sntp broadcast client**

**no sntp broadcast client**

---

### Syntax Description

---

This command has no arguments or keywords.

---

---

### Defaults

By default, the SNTP multicast client is disabled.

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example enables the SNTP multicast client.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#sntp broadcast client
NME-APA(config)#
```

---

### Related Commands

[show sntp](#) (on page 2-206)

[sntp server](#) (on page 2-230)

[sntp update-interval](#) (on page 2-231)

## sntp server

Enables the SNTP uni-cast client to query the specified SNTP server. Use the **no** form of this command to disable the SNTP uni-cast server.

**sntp server** {*address*|*hostname*}

**no sntp server** *hostname*

**no sntp server all**

| Syntax Description |                                                   |
|--------------------|---------------------------------------------------|
|                    | <i>address</i> The IP address of the SNTP server. |
|                    | <i>hostname</i> The hostname of the SNTP server.  |

**Defaults** SNTP uni-cast server is disabled

**Command Modes** Global Configuration  
Use the **all** keyword with the **no** form of this command to disable all SNTP uni-cast servers.

**Usage Guidelines** Authorization: admin

**Examples** The following example enables an SNTP server at a specified IP address.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#sntp server 128.182.58.100
NME-APA(config)#
```

**Related Commands** [show sntp](#) (on page 2-206)  
[sntp broadcast client](#) (on page 2-229)  
[sntp update-interval](#) (on page 2-231)

## sntp update-interval

Defines the interval (in seconds) between SNTP uni-cast update queries.

**sntp update-interval** *interval*

---

### Syntax Description

---

*interval* The interval between queries in seconds.

---

---

### Defaults

interval = 900 seconds

---

### Command Modes

Global Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example sets the SNTP update interval for 100 seconds.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#sntp update-interval 100
NME-APA(config)#
```

---

### Related Commands

[show sntp](#) (on page 2-206)  
[sntp server](#) (on page 2-230)  
[sntp broadcast client](#) (on page 2-229)

## tacacs-server host

Defines a new TACACS+ server host that is available to the NME-APA module TACACS+ client.

Use the **no** form of the command to remove a TACACS+ server host.

The Service Control solution supports a maximum of three TACACS+ server hosts.

**tacacs-server host** *host-name* [**port** *port#*] [**timeout** *timeout-interval*] [**key** *key-string*]

**no tacacs-server host** *host-name*

---

### Syntax Description

*host-name* name of the server

*port #* TACACS+ port number

*timeout-interval* time in seconds that the server waits for a reply from the server host before timing out

*key-string* encryption key that the server and client will use when communicating with each other. Make sure that the specified key is actually configured on the TACACS+ server host.

---



---

### Defaults

Default *port#* = 49

Default *timeout-interval* = 5 seconds or user-configured global default timeout interval

Default *key-string* = no key or user-configured global default key

---

### Command Modes

Global Configuration

---

### Usage Guidelines

The user can configure a global default timeout interval that will be applied as the timeout to all TACACS+ server hosts. The timeout interval then does not need to be configured explicitly for each server. (See [tacacs-server timeout](#) (on page 2-235))

Similarly, the user can configure a global default key that will be applied to all TACACS+ server hosts. (See [tacacs-server key](#) (on page 2-234))

If the global default timeout interval and key string are configured, an explicitly configured value for a specific TACAS+ server overrides the global default for that server.

Authorization: admin

---

**Examples**

The following example shows how to configure a TACACS+ server host using the default port and no key.

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#config  
NME-APA(config)#tacacs-server host server1 timeout 8  
NME-APA(config)#
```

---

**Related Commands**

[tacacs-server key](#) (on page 2-234)

[tacacs-server timeout](#) (on page 2-235)

[show tacacs](#) (on page 2-210)

## tacacs-server key

Defines the global default encryption key for the TACACS+ server hosts.

Use the **no** form of the command to clear the TACACS+ key.

**tacacs-server key** *key-string*

**no tacacs-server key**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>key-string</i> default encryption key that all TACACS servers and clients will use when communicating with each other. Make sure that the specified key is actually configured on the TACACS+ server hosts.                                                                                                                                                                                                                   |
| Defaults           | Default is no encryption                                                                                                                                                                                                                                                                                                                                                                                                         |
| Command Modes      | Global Configuration                                                                                                                                                                                                                                                                                                                                                                                                             |
| Usage Guidelines   | <p>This default key can be overridden for a specific TACACS+ server host by explicitly configuring a different key for that TACACS+ server host.</p> <p>If no global default key is defined, each TACACS+ server host may still have a specific key defined. However, any server host that does not have a key explicitly defined (uses the global default key) is now configured to use no key.</p> <p>Authorization: admin</p> |
| Examples           | <p>The following example show how to configure the keystack.</p> <pre><b>NME-APA&gt;</b>enable 10 <b>NME-APA&gt;</b>Password:&lt;cisco&gt; <b>NME-APA#</b>config <b>NME-APA(config)#</b>tacacs-server key ABCDE <b>NME-APA(config)#</b></pre>                                                                                                                                                                                    |
| Related Commands   | <p><a href="#">tacacs-server host</a> (on page 2-232)</p> <p><a href="#">tacacs-server timeout</a> (on page 2-235)</p> <p><a href="#">show tacacs</a> (on page 2-210)</p>                                                                                                                                                                                                                                                        |

## tacacs-server timeout

Defines the global default timeout interval for the TACACS+ server hosts.

Use the **no** form of the command to clear the global default timeout interval.

**tacacs-server timeout** *timeout-interval*

**no tacacs-server timeout**

---

### Syntax Description

*timeout-interval* default time in seconds that the server waits for a reply from the server host before timing out.

---



---

### Defaults

Default = 5 seconds

---

### Command Modes

Global Configuration

---

### Usage Guidelines

This default timeout interval can be overridden for a specific TACACS+ server host by explicitly configuring a different timeout interval for that TACACS+ server host.

If no global default timeout interval is defined, each TACACS+ server host may still have a specific timeout interval defined. However, any server host that does not have a timeout interval explicitly defined (uses the global default timeout interval) is now configured to a five second timeout interval.

Authorization: admin

---

### Examples

This example shows how to configure a default timeout interval of 10 seconds.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#tacacs-server timeout 10
NME-APA(config)#
```

---

### Related Commands

[tacacs-server host](#) (on page 2-232)

[tacacs-server key](#) (on page 2-234)

[show tacacs](#) (on page 2-210)

## telnet

Starts a Telnet session.

**telnet** *address* [*ports*]

---

### Syntax Description

*address* Telnet access address.

*ports* Optional port number.

---

---

### Defaults

Default port is 23.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example starts a telnet session:

```
NME-APA>enable 10
```

```
Password:<cisco>
```

```
NME-APA#telnet 10.1.5.120
```

```
connecting to 10.1.5.120:23...
```

---

### Related Commands

[show telnet sessions](#) (on page 2-212)

[service telnetd](#) (on page 2-125)

## timeout

Configures the timeout for the Telnet session when the Telnet session is idle. After this time, the Telnet session is disconnected.

Use the **no** form of the command to configure the Telnet server to work with no timeout. No matter how long there is no activity on the Telnet session, the system does not automatically disconnect the Telnet session.

**timeout** *time*

**no timeout**

|                    |                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>time</i> Timeout length in minutes.                                                                                                                                                                                                                                    |
| Defaults           | time = 30 minutes                                                                                                                                                                                                                                                         |
| Command Modes      | Line Configuration Mode                                                                                                                                                                                                                                                   |
| Usage Guidelines   | Authorization: admin                                                                                                                                                                                                                                                      |
| Examples           | <p>The following example sets the timeout to 45 minutes.</p> <pre> <b>NME-APA</b>&gt;enable 10 Password:&lt;cisco&gt; <b>NME-APA</b>#config <b>NME-APA</b>(config)#interface linecard 0 <b>NME-APA</b>(config-line)#<b>timeout</b> 45 <b>NME-APA</b>(config-line)# </pre> |
| Related Commands   | <a href="#">telnet</a> (on page 2-236)                                                                                                                                                                                                                                    |

## tos-marking reset-table

Resets TOS settings to the Diffserv defaults.

### tos-marking reset-table

---

**Syntax Description**

This command has no arguments or keywords.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Linecard Interface Configuration

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example resets the TOS marking.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#tos-marking reset-table
NME-APA(config if)#
```

---

**Related Commands**

[tos-marking set-table-entry](#) (on page 2-239)

[show interface linecard tos-marking table](#) (on page 2-153)

## tos-marking set-table-entry

The NME-APA module supports configuration via CLI of the mapping between the class and coloring and the exposed DSCP (Diffserv Code Points) values. The default of this table is direct mapping of the Diffserv standard code points.

The TOS table reads the class and color of the packet being transmitted, and assigns the value set in the table according to the color and class.

**tos-marking set-table-entry class class color color value value**

### Syntax Description

|              |                                                                                                                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>class</i> | Internal class of service assigned to the packet. Legal values are <b>BE</b> , <b>AF1</b> , <b>AF2</b> , <b>AF3</b> , <b>AF4</b> and <b>EF</b> .                                            |
| <i>color</i> | Internal color assigned to the packet. Legal values are <b>green</b> , <b>yellow</b> , <b>red</b> and <b>any</b> .                                                                          |
| <i>value</i> | Value of the TOS marking, assigned to the packet IP header, as transmitted by the NME-APA module. This is a 6-bit value, expressed as a hex number in the range <b>0x0</b> to <b>0x3f</b> . |

### Defaults

Diffserv defaults

### Command Modes

Linecard Interface Configuration

### Usage Guidelines

Authorization: admin

### Examples

The following example sets a TOS marking table entry.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# tos-marking set-table-entry class AF4 color
yellow value 0x24
NME-APA(config if)#
```

### Related Commands

[show interface linecard tos-marking table](#) (on page 2-153)

[tos-marking reset-table](#) (on page 2-238)

## tracert

Determines the route packets take to reach a specified host.

**tracert** [*hostname*|*IP-address*]

---

### Syntax Description

*hostname* Destination hostname

*IP-address* Destination IP address

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

The destination of the traceroute function can be specified as either a known hostname or an IP address.

Authorization: admin

---

### Examples

Following is a tracert command with sample output.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#tracert 64.103.125.118
traceroute to 10.56.217.103, 30 hops max, 40 byte packets
 1      10.56.217.1 (    10.56.217.1)    0 ms  1 ms  0 ms
 2      10.56.223.9 (    10.56.223.9)    1 ms  0 ms  1 ms
 3      64.103.115.209 ( 64.103.115.209)    0 ms  1 ms  0 ms
 4      64.103.125.118 ( 64.103.125.118)    0 ms  0 ms  0 ms

Trace complete.
NME-APA(config if)#
```

---

### Related Commands

## traffic-counter

Defines a new traffic counter. Use the no form of the command to delete an existing traffic counter.

**traffic-counter name** *name* {**count-bytes** | **count-packets**}

**no traffic-counter** {**name** *name* |**all**}

---

### Syntax Description

---

*name* Name to be assigned to this traffic counter.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

The following are usage guidelines for the **traffic-counter** command:

- Use the **count-bytes** keyword to enable counting the bytes in each packet.  
The counter will increment by the number of bytes in each packet.
- Use the **count-packets** keyword to enable counting whole packets.  
The counter will increment by one for each packet.

Use the **all** keyword with the **no** form to delete all existing traffic counters.

Authorization: admin

---

### Examples

The following are examples of the **traffic-counter** command:

**EXAMPLE 1:**

Following is an example of creating a traffic counter that will count bytes.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#traffic-counter name counter1 count-bytes
NME-APA(config if)#
```

**EXAMPLE 2:**

The following example demonstrates how to delete all traffic counters.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#no traffic-counter all
NME-APA(config if)#
```

---

**Related Commands**

*show interface linecard traffic-counter* (on page 2-154)

*clear interface linecard traffic-counter* (on page 2-26)

## traffic-rule

Defines a new traffic rule. Use the **no** form of the command to delete an existing traffic rule.

**traffic-rule name** *name* **ip addresses** *ip-addresses* **protocol** *protocol* [**tunnel-id** *tunnel-id*]  
**direction** *direction* **traffic-counter name** *traffic-counter* **action** *action*

**traffic-rule tunnel-id-mode**

**no traffic-rule** {**name** *name* |**all**|**tunnel-id-mode**}

### Syntax Description

|                        |                                                                                        |
|------------------------|----------------------------------------------------------------------------------------|
| <i>name</i>            | name to be assigned to this traffic rule.                                              |
| <i>IP-addresses</i>    | user-side and network-side <IP specification> (see below)                              |
| <i>protocol</i>        | Any one of the following protocols:<br><i>TCP/UCP/ICMP/IGRP/EIGRP/IS-IS/OSPF/Other</i> |
| <i>tunnel-id</i>       | Tunnel ID, <tunnel Id specification> (see below).                                      |
| <i>direction</i>       | upstream/downstream/both                                                               |
| <i>traffic-counter</i> | name of traffic counter/none                                                           |
| <i>action</i>          | action to be performed on flows that meet the rule criteria (see below)                |

### Defaults

This command has no default settings.

### Command Modes

Linecard Interface Configuration

### Usage Guidelines

The following are the usage guidelines for the **traffic-rule** command:

#### IP specification:

all([all-but] (<ip-address>|<ip-range>))

- <ip-address> is a single IP address in dotted-decimal notation, such as 10.1.2.3
- <ip-range> is an IP subnet range, in the dotted-decimal notation followed by the number of significant bits, such as 10.1.2.0/24.

#### tunnel id specification:

all([all-but] tunnel id)

- tunnel id is a Hex Tunnel id range, in the format '(HEX)Tunnel-id' or '(HEX)MinTunnelId:(HEX)MaxTunnelId'

**traffic-counter name:**

Either of the following:

- *Name of an existing traffic counter:* Packets meeting the criteria of the rule are to be counted in the specified counter. If a counter name is defined, the “count” action is also defined implicitly.
- *none:* If **none** is specified, then an action must be explicitly defined via the **action** option.
- Use the **all** keyword with the no form to delete all existing traffic rules.
- Use the **tunnel-id-mode** keyword to enable or disable defining the traffic rule according to the tunnel ID.

**action:**

One of the following:

- **block** — Block the specified traffic; this option is not currently supported.
- **ignore** — Bypass the specified traffic; traffic receives no service
- **quick-forwarding** — Quick forwarding (duplication) of delay-sensitive packets with service.
- **quick-forwarding-ignore** — Quick forwarding (duplication) of delay-sensitive packets with no service.

Authorization: admin

**Examples**

The following examples illustrate how to use this command.

**EXAMPLE 1:**

This example creates the following traffic rule:

Name = rule2

IP addresses: user side = all IP addresses, network side = all IP addresses EXCEPT the subnet 10.10.10.0/24

Protocol = TCP

Direction = downstream

Traffic counter = counter2

Action = Block

The actions performed will be counting and blocking

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA (config if)# traffic-rule name rule2 ip-addresses user-
side all network-side all-but 10.10.10.0/24 protocol tcp
direction downstream traffic-counter name counter2 action block
NME-APA(config if)
```

**EXAMPLE 2:**

This example creates the following traffic rule:

Name = rule3

IP addresses: all

Protocol = IS-IS

Direction = upstream

Traffic counter = none

Action = ignore (required since traffic-counter = none)

The only action performed will be **Ignore**.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA (config if)# traffic-rule name rule3 ip-addresses all
protocol is-is direction upstream traffic-counter name none
action ignore
NME-APA(config if)
```

**EXAMPLE 3:**

The following example demonstrates how to delete all traffic rules.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#no traffic-rule all
NME-APA(config if)
```

---

Related Commands

[show interface linecard traffic-rule](#) (on page 2-155)

## unzip

Extracts a zip file to the current directory.

**unzip** *filename*

---

**Syntax Description**

---

*filename* Zip file to be extracted.

---

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC

---

**Usage Guidelines**

Authorization: admin

---

**Examples**

The following example extracts the zipfile.zip:

```
NME-APA>enable 10
Password:<cisco>
NME-APA#unzip zipfile.zip
Unzipping '/tffs0/zipfile.zip'...
Zip file has 3 entries:
  1.sli, 13429 bytes extracted
  preflut.sli, 12558 bytes extracted
  temp/SLI/x/IpraeLut.sli, 12929 bytes extracted
Finished, Extracted 3 files.
```

---

**Related Commands**

## user anonymous-group export csv-file

Exports anonymous groups to the specified csv file.

**user anonymous-group export csv-file** *filename*

---

### Syntax Description

---

*filename* Name of the csv file to which the anonymous groups information is to be exported.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example exports anonymous groups information to the specified file

```
NME-APA>enable 10  
Password:<cisco>  
NME-APA#config  
NME-APA(config)#interface linecard 0  
NME-APA(config if)# user anonymous-group export csv-file  
s_g_0507.csv  
NME-APA(config if)#
```

---

### Related Commands

[user anonymous-group import csv-file](#) (on page 2-248)

## user anonymous-group import csv-file

Creates anonymous groups by importing anonymous users from the specified csv file.

**user anonymous-group import csv-file** *filename*

---

|                    |                                                                                          |
|--------------------|------------------------------------------------------------------------------------------|
| Syntax Description | <i>filename</i> Name of the <i>csv</i> file containing the anonymous groups information. |
|--------------------|------------------------------------------------------------------------------------------|

---

|          |                                       |
|----------|---------------------------------------|
| Defaults | This command has no default settings. |
|----------|---------------------------------------|

|               |                                  |
|---------------|----------------------------------|
| Command Modes | Linecard Interface Configuration |
|---------------|----------------------------------|

|                  |                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | Anonymous Group <i>csv</i> files have a fixed format. All lines have the same structure, as described below: |
|------------------|--------------------------------------------------------------------------------------------------------------|

Anonymous-group-name, IP-range [, user-template-number].

If no user-template-number is specified, then the anonymous users of that group will use the default template (#0), which cannot be changed by template import operations.

Following is an example of an anonymous group *csv* file:

```
group1, 10.1.0.0/16, 2
group2, 176.23.34.0/24, 3
group3, 10.2.0.0/16
```

Authorization: admin

|          |                                                                                                                                                                                                                                                                                                                                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Examples | <p>The following example imports user from the file <i>users_groups.csv</i>.</p> <pre><b>NME-APA</b>&gt;enable 10 Password:&lt;cisco&gt; <b>NME-APA</b>#config <b>NME-APA</b>(config)#interface linecard 0 <b>NME-APA</b>(config if)# <b>user anonymous-group import csv-file</b> <b>users_groups.csv</b> <b>NME-APA</b>(config if)#</pre> |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                  |                                                                      |
|------------------|----------------------------------------------------------------------|
| Related Commands | <a href="#">user anonymous-group export csv-file</a> (on page 2-247) |
|------------------|----------------------------------------------------------------------|

## user export csv-file

Exports users to the specified csv file. User csv files are application-specific. Refer to the relevant application documentation for the definition of the file format.

**user export csv-file** *filename*

---

### Syntax Description

---

*filename* Name of the *csv* file to which the user information is to be exported.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

User *csv* files are application-specific. Refer to the relevant application documentation for the definition of the file format.

Authorization: admin

---

### Examples

The following example exports users to the specified file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# user export csv-file gold_users_04072003.csv
NME-APA(config if)#
```

---

### Related Commands

[user import csv-file](#) (on page 2-250)

## user import csv-file

Imports users from the specified csv file.

**user import csv-file** *filename*

---

### Syntax Description

*filename* Name of the *csv* file containing the user information.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

User *csv* files are application-specific. Refer to the relevant application documentation for the definition of the file format.

Authorization: admin

---

### Examples

The following example imports user from the file *gold\_users.csv*.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# user import csv-file gold_users.csv
NME-APA(config if)#
```

---

### Related Commands

[user export csv-file](#) (on page 2-249)

## user name property

Assigns a value to the specified property of the specified user.

**user name** *user-name* **property** *propertyname* **value** *property-val*

---

### Syntax Description

*user-name* Name of the user.

*propertyname* The user property for which the value is to be assigned

*property-val* The value to be assigned

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

This command can be used to enable or disable the generation of the real-time user usage RDRs (see example below).

To enable RDR generation, set *propertyname* = monitor and *property-val* = 1

To disable RDR generation, set *propertyname* = monitor and *property-val* = 0

To enable user monitoring for a group of users, create a text file containing the sequence of CLI commands, including the commands to access the appropriate CLI mode. The file would look something like this:

```
configure
interface linecard 0
user name Jerry property monitor value 1
user name George property monitor value 1
user name Elaine property monitor value 1
user name Kramer property monitor value 1
user name Newman property monitor value 1
```

Use the [script run](#) (on page 2-121) command to run the script.

Authorization: admin

---

**Examples**

The following example disables the generation of the real-time user usage RDRs for user jane\_smith.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#user name jane_smith property monitor value 0
NME-APA(config if)#
```

---

**Related Commands**

*show interface linecard user name* (on page 2-165)

## user template export csv-file

Exports a user template to the specified csv file, according to the party template.

**user template export csv-file** *filename*

---

### Syntax Description

---

*filename* Name of the *csv* file to which the user template is to be exported.

---

---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example exports the user template to the specified file.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# user template export csv-file gold0507.csv
NME-APA(config if)#
```

---

### Related Commands

[user template import csv-file](#) (on page 2-254)

## user template import csv-file

Imports a user template from the specified csv file, creating a party template.

**user template import csv-file** *filename*

---

### Syntax Description

*filename* Name of the *csv* file containing the user template.

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

Authorization: admin

---

### Examples

The following example imports the user template from the file *gold0507.csv*.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)# user template import csv-file gold0507.csv
NME-APA(config if)#
```

---

### Related Commands

[user template export csv-file](#) (on page 2-253)

## user aging

Enables/disables user aging for the specified type of users (anonymous or introduced).

The aging period may also be defined when aging is enabled.

**user aging anonymous|introduced [timeout *aging-time*]**

**no user aging anonymous|introduced**

---

### Syntax Description

*aging-time* In minutes.

*anonymous* Anonymous groups users

*introduced* Introduced users

---



---

### Defaults

This command has no default settings.

---

### Command Modes

Linecard Interface Configuration

---

### Usage Guidelines

The most common usage for aging is for anonymous users, since this is the easiest way to ensure that anonymous users who have logged-out of the network are removed from the NME-APA module and are no longer occupying resources. Aging time can be configured individually for introduced users and for anonymous users.

Authorization: admin

---

### Examples

The following example enables user aging for anonymous users with a timeout period of 10 minutes.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#interface linecard 0
NME-APA(config if)#user aging anonymous timeout 10
NME-APA(config if)#
```

---

### Related Commands

[show interface linecard user aging](#) (on page 2-158)

## username

Adds a new user to the local database

Use the **no** form of the command to remove a user from the database.

**username** *name* { **password** *password* | **nopassword** | **secret** { **0** *password* | **5** *password* } }

**no username** *name*

### Syntax Description

|                 |                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>     | name of the user to be added                                                                                                                  |
| <i>password</i> | a clear text password.                                                                                                                        |
| <i>secret</i>   | the password is saved in MD5 encrypted form. The keywords <b>0</b> or <b>5</b> indicate the format of the password as entered in the command: |

### Defaults

### Command Modes

Global Configuration

### Usage Guidelines

Up to 100 users may be defined.

The password is defined with the username. There are several password options:

- **No password:** use the *nopassword* keyword.
- **Password:** Password is saved in clear text format in the local list.  
Use the *password* parameter.
- **Encrypted password:** Password is saved in encrypted (MD5) form in the local list. Use the *secret* keyword and either of the following options.

Password may be defined by either of the following methods:

- Specify a clear text password, which is saved in MD5 encrypted form
- Specify an MD5 encryption string, which is saved as the user MD5-encrypted secret password

The following keywords are available:

- **nopassword:** There is no password associated with this user
- **secret:** the password is saved in MD5 encrypted form. Use with either of the following keywords to indicate the format of the password as entered in the command:
  - **0:** the *<password>* parameter specifies a clear text password that will be saved in MD5 encrypted form
  - **5:** the *<password>* parameter specifies an MD5 encryption string that will be saved as the user MD5-encrypted secret password

Authorization: admin

The following examples illustrate how to use this command.

---

**Examples****EXAMPLE 1**

This example shows how to add a new user to the local database with a clear text password.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#username johndoe password mypassword
NME-APA(config)#
```

**EXAMPLE 2**

This example shows how to add a new user to the local database with no password.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#username johndoe nopassword
NME-APA(config)#
```

**EXAMPLE 3**

This example shows how to add a new user to the local database with with an MD5 encrypted password entered in clear text.

```
NME-APA>enable 10
Password:<cisco>
NME-APA#config
NME-APA(config)#username johndoe secret 0 mypassword
NME-APA(config)#
```

---

**Related Commands**

[show users](#) (on page 2-215)





# Index

?

? • 2-2

## A

aaa accounting commands • 2-3  
aaa authentication attempts • 2-4  
aaa authentication enable default • 2-5  
aaa authentication login default • 2-7  
application slot replace force completion • 2-8  
Argument Help • 1-12  
attack-detector • 2-11  
attack-detector <number> • 2-12  
attack-detector default • 2-9  
attack-detector tcp-port-list|udp-port-list • 2-15  
attack-filter (Linecard Interface Configuration) • 2-16  
attack-filter (Privileged Exec) • 2-18  
attack-filter user-notification ports • 2-20  
Audience • ix  
Authorization and Command Levels (Hierarchy) • 1-2

## B

bandwidth • 2-21

## C

calendar set • 2-22  
cd • 2-23  
Cisco.com • xii  
clear arp-cache • 2-24  
clear interface linecard • 2-25  
clear interface linecard traffic-counter • 2-26  
clear interface linecard user • 2-27  
clear interface linecard user db counters • 2-28

clear logger • 2-29  
clear management-agent notifications counters • 2-31  
clear rdr-formatter • 2-32  
CLI Authorization Levels • 1-5  
CLI Command Hierarchy • 1-3  
CLI Command Reference • 2-1  
CLI Commands • 2-2  
CLI Help Features • 1-11  
CLI Scripts • 1-16  
clock read-calendar • 2-33  
clock set • 2-34  
clock summertime • 2-35  
clock timezone • 2-39  
clock update-calendar • 2-40  
Command History • 1-13  
Command-Line Interface • 1-1  
configure • 2-41  
Configuring the Physical Ports • 1-9  
Contacting TAC by Telephone • xiii  
Contacting TAC by Using the Cisco TAC Website • xiii  
Conventions • x  
copy • 2-42  
copy ftp  
// • 2-43  
copy running-config startup-config • 2-45  
copy source-file ftp  
// • 2-46  
copy source-file startup-config • 2-47  
copy startup-config destination-file • 2-48  
copy-passive • 2-44

## D

default user template all • 2-49  
delete • 2-50  
dir • 2-51  
disable • 2-52

do • 2-53  
 Document Revision History • ix  
 Documentation CD-ROM • xi  
 Documentation Feedback • xii

**E**

enable • 2-54  
 enable password • 2-55  
 Entering and Exiting Global Configuration Mode • 1-8  
 Entering LineCard Interface Configuration Mode • 1-9  
 Entering the Fast Ethernet Line Interface Configuration Mode • 1-10  
 erase startup-config-all • 2-56  
 exit • 2-57  
 Exiting Modes • 1-7

**F**

failure-recovery operation-mode • 2-59  
 Filtering Command Output • 1-15  
 force failure-condition • 2-60  
 FTP User Name and Password • 1-14

**G**

Getting Help • 1-1

**H**

help • 2-61  
 history • 2-63  
 history size • 2-64  
 hostname • 2-65

**I**

Interface Configuration Modes • 1-9  
 interface fastethernet • 2-66  
 interface linecard • 2-67  
 ip advertising • 2-68  
 ip domain-lookup • 2-70  
 ip domain-name • 2-71  
 ip filter fragment • 2-72  
 ip filter monitor • 2-73  
 ip ftp password • 2-75  
 ip ftp username • 2-76  
 ip host • 2-77  
 ip name-server • 2-78  
 ip radius-client retry limit • 2-79  
 ip rpc-adapter • 2-80  
 ip rpc-adapter port • 2-81  
 ip rpc-adapter security-level • 2-82

**K**

Keyboard Shortcuts • 1-13

**L**

line vty • 2-83  
 link mode • 2-84  
 logger add-user-message • 2-86  
 logger device • 2-87  
 logger device user-file-log max-file-size • 2-88  
 logger get support-file • 2-89  
 logger get user-log file-name • 2-90  
 logout • 2-91

**M**

management-agent sce-api logging • 2-92  
 management-agent sce-api timeout • 2-93  
 management-agent system • 2-94  
 Managing Command Output • 1-15  
 mkdir • 2-95  
 more • 2-96  
 more user-log • 2-98

**N**

Navigating Between Configuration Modes • 1-8  
 Navigating between the Interface Configuration Modes • 1-10  
 Navigational and Shortcut Features • 1-13  
 no user • 2-99  
 no user anonymous-group • 2-100  
 no user mappings included-in • 2-101

**O**

Obtaining Documentation • xi  
 Obtaining Technical Assistance • xii  
 Ordering Documentation • xi  
 Organization • x

**P**

Partial Help • 1-11  
 ping • 2-102  
 pqi install file • 2-103  
 pqi rollback file • 2-104  
 pqi uninstall file • 2-105  
 pqi upgrade file • 2-106  
 Preface • ix  
 Prompt Indications • 1-7  
 pwd • 2-107



show system operation-status • 2-208  
 show system-uptime • 2-209  
 show tacacs • 2-210  
 show telnet sessions • 2-212  
 show telnet status • 2-213  
 show timezone • 2-214  
 show users • 2-215  
 show version • 2-216  
 show version all • 2-218  
 show version software • 2-220  
 silent • 2-221  
 snmp-server • 2-222  
 snmp-server community • 2-223  
 snmp-server contact • 2-224  
 snmp-server enable traps • 2-225  
 snmp-server host • 2-227  
 snmp-server location • 2-228  
 snmp broadcast client • 2-229  
 snmp server • 2-230  
 snmp update-interval • 2-231  
 Syntax and Conventions • 2-1

## T

Tab Completion • 1-14  
 tacacs-server host • 2-232  
 tacacs-server key • 2-234  
 tacacs-server timeout • 2-235  
 Technical Assistance Center • xiii  
 telnet • 2-236  
 The • 1-11  
 The [no] Prefix • 1-12  
 timeout • 2-237  
 tos-marking reset-table • 2-238  
 tos-marking set-table-entry • 2-239  
 tracer • 2-240  
 traffic-counter • 2-241  
 traffic-rule • 2-243

## U

unzip • 2-246  
 user aging • 2-255  
 user anonymous-group export csv-file • 2-247  
 user anonymous-group import csv-file • 2-248  
 user export csv-file • 2-249  
 user import csv-file • 2-250  
 user name property • 2-251  
 user template export csv-file • 2-253  
 user template import csv-file • 2-254

username • 2-256

## W

World Wide Web • xi