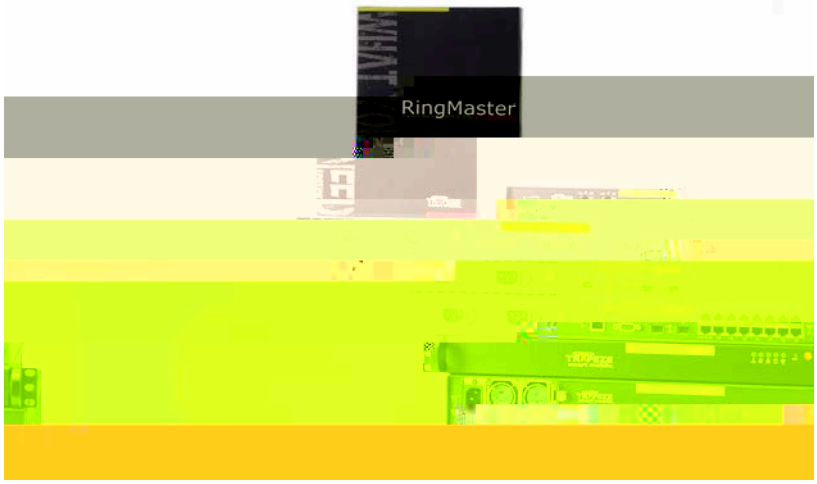
™


RingMaster

Information to Have Available

To expedite your service request, have the following information available when you call or write to TAC for technical assistance:

- Your company name and address
- Your name, telephone number, cell phone or pager number, and e–mail address
- Name, model, and serial number of the product(s) requiring service
- Software version and release number
- Output of the **show tech-support** command
- Wireless client information
- License levels for RingMaster™ and Mobility Exchange™ (MX™) products
- Description of the problele

(c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification or (e) is provided to Customer for pre-production, evaluation or charitable purposes.

4. Limited Software Warranty

Trapeze Networks warrants to Customer, subject to the limitation and disclaimer below, that the software will substantially conform to its published specifications as follows: (a) if the software was purchased directly from Trapeze Networks, for a period of ninety (90) days after original shipment by Trapeze Networks to Customer or (b) if the software was purchased from a Trapeze Networks Authorized Reseller, for a period of ninety (90) days from the date of delivery to Customer commencing not more than ninety (90) days after original shipment date by Trapeze), ("Limited Hardware Warranty"). The date of original shipment from Trapeze Networks will be determined by shipping evidence on file at Trapeze Networks. This Limited Software Warranty extends only to the Customer of original purchaser of the software and may not be transferred to any subsequent repurchasing entity.

During the Limited Software Warranty period upon proper notice to Trapeze Networks by

Customer, Trapeze Networks will, at its option, either:

a. Use reasonable commercial efforts to attempt to correct or provide workarounds for errors;

b. Replace the software with functionally equivalent software; or

c. Refund to Customer the license fees paid by Customer for the software.

Trapeze Networks does not warrant or represent that the software is error free or that the software will operate without problems or disruptions. Additionally, and due to the steady and ever-improving development of various attack and intrusion technologies, Trapeze Networks does not warrant or represent that any networks, systems or software provided by Trapeze Networks will be free of all possible methods of access, attack or intrusion.

5. Restrictions on the Limited Software Warranty

This Limited Software Warranty does not apply if software (a) is altered in any way from its specifications, (b) is installed, configured, implemented or operated in any way that is contrary to its documentation, (c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification, or (e) is provided to Customer for pre-production, evaluation or charitable purposes.

6. General Warranty Disclaimer

EXCEPT AS SPECIFIED IN THIS LIMITED WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR APPLICATION OR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE AFOREMENTIONED WARRANTY PERIOD. BECAUSE SOME STATES, COUNTRIES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED

LIABLE FOR ANY MONETARY OR PUNITIVE DAMAGES ARISING OUT OF THE USE OF, OR INABILITY TO USE TRAPEZE NETWORKS HARDWARE OR SOFTWARE. TRAPEZE NETWORKS' LIABILITY SHALL NOT EXCEED THE PRICE PAID BY THE CUSTOMER FOR ANY HARDWARE OR SOFTWARE COVERED UNDER THE TERMS AND CONDITIONS OF THIS WARRANTY. THIS LIMITATION OF LIABILITY AND RESTRICTION ON DAMAGES APPLIES WHETHER IN CONTRACT, TORT, NEGLIGENCE, OR OTHERWISE, AND SHALL APPLY EVEN IF THE LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. WARRANTY LAWS VARY FROM JURISDICTION TO JURISDICTION, AND THE ABOVE LIMITATIONS AND EXCLUSION OF CONSEQUENTIAL AND INCIDENTAL DAMAGES MAY NOT APPLY TO YOU, DEPENDING UPON YOUR STATE, COUNTRY OR JURISDICTION.

8. Procedures for Return of Hardware or Software under the Limited Warranty

Where repair or replacement is required under the Limited Warranty, Customer will contact Trapeze Networks and obtain a Return Materials Authorization number ("RMA Number") prior to returning any hardware and/or so

The Mobility System Software (MSS™) documentation set describes configuring and managing the Trapeze Networks Mobility System™ wireless LAN (WLAN) using command line interface (CLI) commands that you ente

- — Instructions for managing and monitoring your WLAN using the RingMaster tool suite and how to optimize and manage your WLAN.

- — Instructions and specifications for installing an MX switch
- — Instructions for performing basic setup of secure (802.1X) and guest (WebAAA™) access, and for configuring a Mobility Domain for roaming
- — Instructions and specifications for installing an MP access point and connecting it to an MX.
- — Instructions and specifications for installing the MP-620 access point and connecting to an MX.
- — Important safety instructions and compliance information that you must read before installing Trapeze Networks products.

- — Instructions for planning, configuring, deploying, and managing the entire WLAN with the RingMaster tool suite
- — Instructions for configuring advanced features through the MSS CLI.
- — Instructions for configuring and managing the system through the MSS CLI.
- — Functional and alphabetic reference to all MSS commands supported on MX switches and MPs.

The following kinds of safety and advisory notices appear in this manual.

Hypertext links appear in Blue.
As an example, this is a link to **Contacting the Technical Assistance Center**.

Trapeze guides use the following text and syntax conventions:

.

TERMS AND CONDITIONS OF SALE

1. Software

Any software provided is licensed pursuant to the terms of Trapeze Networks' Software License Agreement, an electronic copy of which is provided with the Software and a printed copy of which is available upon request. The terms and conditions of the Software License Agreement are incorporated herein in its entirety in this Terms and Conditions of Sale ("Terms and Conditions of Sale") by this reference. The terms of the Software License Agreement control, except for the limited warranty set forth below ("Limited Warranty").

2. Limited Hardware Warranty

Trapeze Networks, Inc. ("Trapeze Networks" or "Trapeze") warrants to Customer, subject to the limitation and disclaimer below, that all Trapeze hardware will be free from defects in material and workmanship under normal use as follows: (a) if the hardware was purchased directly from Trapeze Networks, for a period of one (1) year after original shipment by Trapeze Networks to Customer or (b) if the hardware was purchased from a Trapeze Networks Authorized Reseller, for a period of one (1) year from the date of delivery to Customer, but in no event more than fifteen (15) months after the original shipment date by Trapeze ("Limited Hardware Warranty").
The date of original shipment from Trapeze Networks will be determined by shipping evidence on file at Trapeze Networks. This Limited Hardware Warranty extends only to the Customer who was the original purchaser of the hardware and may not be transferred to any subsequent repurchasing entity. During the Limited Hardware Warranty period upon proper notice to Trapeze Networks by Customer, Trapeze Networks will, at its sole option, either:

- ❍ Repair and return of the defective hardware;
- ❍ Replace the defective hardware with a new or refurbished component;
- ❍ Replace the defective hardware with a different but similar component that contains compatible features and functions; or
- ❍ Refund the original purchase price upon presentation of proof of purchase to Trapeze Networks.

3. Restrictions on the Limited Hardware Warranty.

This Limited Warranty does not apply if hardware (a) is altered from its original specifications, (b) is installed, configured, implemented or operated in any way that is contrary to its documentation, (c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification or (e) is provided to Customer for pre-production, evaluation or charitable purposes.

4. Limited Software Warranty

Trapeze Networks warrants to Customer, subject to the limitation and disclaimer below, that the software will substantially conform to its published specifications as follows: (a) if the software was purchased directly from Trapeze Networks, for a period of ninety (90) days after original shipment by Trapeze Networks to Customer or (b) if the software was purchased from a Trapeze Networks Authorized Reseller, for a period of ninety (90) days from the date of delivery to Customer commencing not more than ninety (90) days after original shipment date by Trapeze), ("Limited Hardware Warranty"). The date of original shipment from Trapeze

LIMITATIONS AND EXCLUSION OF CONSEQUENTIAL AND INCIDENTAL DAMAGES MAY NOT APPLY TO YOU, DEPENDING UPON YOUR STATE, COUNTRY OR JURISDICTION.

8. Procedures for Return of Hardware or Software under the Limited Warranty

Where repair or replacement is required under the Limited Warranty, Customer will contact Trapeze Networks and obtain a Return Materials Authorization number ("RMA Number") prior to returning any hardware and/or software, and will include the Trapeze Networks RMA Number on all packaging. Trapeze Networks will ship repaired or replacement components within a commercially reasonable time after receipt of any hardware and/or software returned for the Limited Warranty purposes to the address provided by Customer. Customer will pay freight and handling charges for defective return to the address specified by Trapeze Networks and Trapeze Networks will pay freight and handling charges for return of the repair or replacement materials to Customer.

9. Miscellaneous

The Limited Warranty shall be governed by and construed in accordance with the laws of the State of California without reference to that State's conflict of laws rules and as if the contract was wholly formed within the State of California. Customer agrees that jurisdiction and venue shall be in Santa Clara County, California. Under no circumstances shall the United Nations Convention on the International Sale of Goods be considered for redress of grievances or adjudication of any warranty disputes that include Trapeze Networks hardware or software. If any provision of these Terms and Conditions of Sale are held invalid, then the remainder of these Terms and Conditions of Sale will continue in full force and effect. Where a Customer has entered into a signed contractual agreement with Trapeze Networks for supply of hardware, software or services, the terms of that agreement shall supersede any terms contained within this Limited Warranty. Customer understands and acknowledges that the terms of this Limited Warranty, as well as material information regarding the form, function, operation and limitations of Trapeze Networks hardware and software will change from time to time, and that the most current revisions will be publicly available at the Trapeze Networks corporate web site (www.trapezenetworks.com).

Mobility System Software (MSS) operates a Trapeze Networks Mobility System wireless LAN (WLAN) consisting of RingMaster software, Mobility Exchange (MX) switches, and Mobility Point

- Italic monospace font indicates a placeholder for a value. For example, you replace in the following command with a virtual LAN (VLAN) ID:

```
[illegible]
```

- Curly brackets ({ }) indicate a mandatory parameter, and square brackets ([ ]) indicate an optional parameter. For example, you must enter **dynamic** or **port** and a port list in the following command, but a VLAN ID is optional:

```
[illegible]
```

- A vertical bar (|) separates mutually exclusive options within a list of possibilities. For example, you enter either enable or disable, not both, in the following command:

```
[illegible]
```

Unless otherwise indicated, the MSS CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

Trapeze Networks recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names and .

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks (“”).

In addition, the CLI does not support the use of international characters such as the accented in DÉCOR.

MSS displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes—for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (:) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. MAC addresses are displayed including all leading zeros.
- In some specified commands, you can use the single-asterisk (*) wildcard character to represent an entire MAC address or from 1 byte to 5 bytes of the address.

MSS displays IP addresses in dotted decimal notation—for example, 192.168.1.111. MSS uses both subnet masks and wildcard masks.

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks—for example, 192.168.1.11

The ACL mask must be a contiguous set of zeroes starting from the first bit. For example, 0.255.255.255, 0.0.255.255, and 0.0.0.255 are valid ACL masks. However, 0.255.0.255 is not a valid ACL mask.

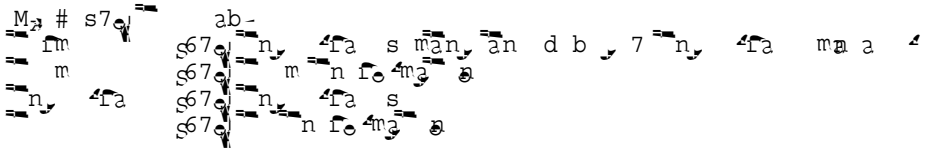
The physical Ethernet ports on an MX can be set for MP connections, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one MSS CLI command by using the appropriate list format.

The ports on an MX are numbered 1 through 22. No port 0 exists on the MX. You can include a

Ctrl+P or Up Arrow key	Enters the previous command line in the history buffer.
Ctrl+U or Ctrl+X	Deletes characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes characters from the cursor forward to the end of the word.
Delete key or Backspace key	Erases mistake made during command entry. Reenter the command after using this key.

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

The MSS CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to display the command(s) that begin with those characters. For example:



You can use the single-asterisk (*) wildcard character when configuring user globs.

Double-Asterisk (**) Wildcard Characters

The double-asterisk (**) wildcard character matches all usernames.

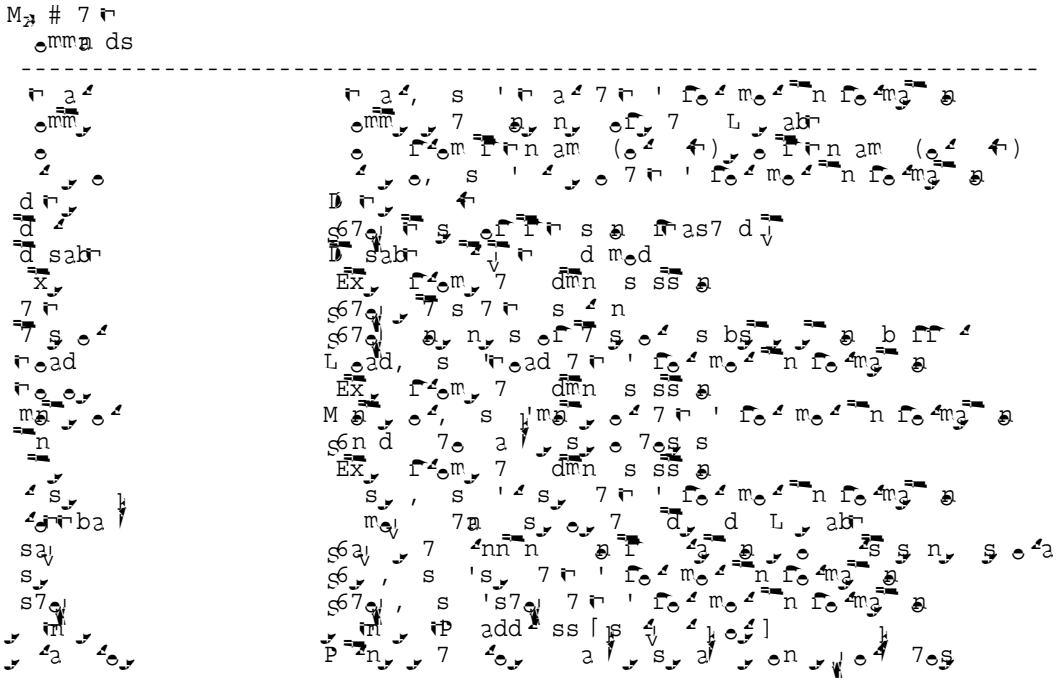
“Globbing” is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. MSS accepts user globs, MAC address globs, and VLAN globs. The order that globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match usernames. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the (@) sign and the period (.).

For example, the following globs identify the following users:

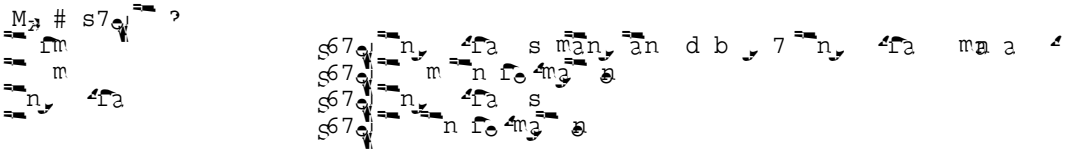
The CLI provides online help. To see the full range of commands available at your access level, type the following command:



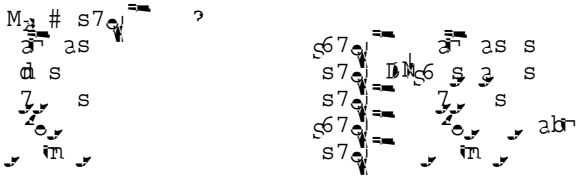
For more information on help, see the help command description in the

.

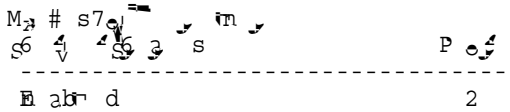
To see a subset of the online help, type the first letter of the command to see more information. For example, the following command displays all the commands that begin with the letter :



To see all the variations, type one of the commands followed by a question mark (?). For example:



To determine the port on which Telnet is running, type the following command:



Use access commands to control access to the Mobility Software System (MSS) (CLI). This chapter presents access commands alphabetically. Use the following table to locate commands in this chapter based on their use.

disable

Changes the CLI session from enabled mode to restricted access.

Syntax **disable**

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Examples The following command restricts access to the CLI for the current session:

```
MX# disable
MX>
```

See Also **enable** on page 3-15

enable

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

Syntax **enable**

Access All.

History Introduced in MSS 1.0.

Usage MSS displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this MX with the **set enablepass** command.

Examples The following command plus the enable password provides enabled access to the CLI for the current sessions:

```
MX> enable
Enter password: password
MX#
```

See Also

- **set enablepass** on page 3-16

- **set confirm** on page 4-26

quit

Exit from the CLI session.

Syntax **quit**

Defaults None.

Access All.

History Introduced in MSS 1.0.

Examples To end your session, type the following command:

```
MX> quit
```

set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the MX switch.

Syntax **set enablepass**

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Usage After typing the **set enablepass** command, press Enter. If you are entering the first enable password on this MX, press Enter at the prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the prompt.

Examples The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

```
MX# set enablepass

Enter old password: old-password
Enter new password: new-password
Retype new password: new-password
Password changed
```

See Also

- **disable** on page 3-15
- **enable** on page 3-15

Use system services commands to configure and monitor system information for a Mobility Exchange (MX) switch. This chapter presents system services commands alphabetically. Use the following table to located commands in this chapter based on their use.

Configuration	**quickstart** on page 4-23
Auto-Config	**set auto-config** on page 4-23
Display	**clear banner motd** on page 4-19
	set banner motd on page 4-25
	set banner acknowledge on page 4-24
	show banner motd on page 4-35
	set confirm on page 4-26
	set length on page 4-27
System Identification	**set prompt** on page 4-28
	set system name on page 4-35
	set system location on page 4-34
	set system contact on page 4-29
	set system countrycode on page 4-29
	set system idle-timeout on page 4-33
	set system ip-address on page 4-34
	show load on page 4-37
	show system on page 4-40
	clear system on page 4-21
	clear prompt on page 4-20
Help	**help** on page 4-22
History	**history** on page 4-22
	clear history on page 4-20
License	**set license** on page 4-27
	show license on page 4-35

clear banner motd

Deletes the message-of-the-day (MOTD) banner that is displayed before the login prompt for each CLI session on the MX switch.

Syntax `clear banner motd`

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples To clear a banner, type the following command:

```
MX# clear banner motd
success: change accepted
```

See Also

- **set banner motd** on page 4-25
- **show banner motd** on page 4-35

clear history

Deletes the command history buffer for the current CLI session.

Syntax **clear history**

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples To clear the history buffer, type the following command:

```
MX# clear history
success: command buffer was flushed.
```

See Also **history** on page 4-22

clear prompt

Resets the system prompt to its previously configured value. If the prompt was not configured previously, this command resets the prompt to the default.

Syntax **clear prompt**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples To reset the prompt, type the following command:

```
wildebeest# clear prompt
success: change accepted.
MX#
```

See Also **set prompt** on page 4-28. (For information about default prompts, see **"Command Prompts" on page 2–5**.)

clear system

Clears the system configuration of the specified information.

Syntax **clear system** [**contact** | **countrycode** | **idle-timeout** | **ip-address** | **location** | **name**]

Defaults None.

Access Enabled.

History

Examples To clear the location of the MX, type the following command:

```
MX# clear system location
success: change accepted.
```

See Also

- **set system contact** on page 4-29
- **set system countrycode** on page 4-29
- **set system idle-timeout** on page 4-33
- **set system ip-address** on page 4-34
- **set system location** on page 4-34
- **show config**

help

Displays a list of commands that can be used to configure and monitor the MX.

Syntax **help**

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To display a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

```
MX# help
Commands:
------------------------------------------------------------------------
backup                Backup system information to filename (or url)
clear                 Clear,  use 'clear help' for more information
commit                Commit the content of the ACL table
copy                  Copy from filename (or url) to filename (or url)
crypto                Crypto, use 'crypto help' for more information
delete                Delete url
dir                   Show list of files on flash device
disable               Disable privileged mode
exit                  Exit from the Admin session
help                  Show this help screen
history               Show contents of history substitution buffer
hit-sample-rate       Set NP hit-counter sample rate
load                  Loah(he)-6(06 Tw6(for)-6((m hae)]TJ-6(p' )6(f)-r)-6(mmonitore )6(i)(for)-6(mati)-6(on)]TJ0
hittentry sSh
```

Syntax **set banner acknowledge mode** {**enable** | **disable**}

Syntax **set banner acknowledge message** **"***message***"**

enable	Enables the prompt to acknowledge the MOTD banner.
disable	Disables the prompt to acknowledge the MOTD banner.
"	Delimiting character that begins and ends the prompt message; for example, double quotes (**"**).
	Up to 32 alphanumeric characters, but the delimiting character.

Defaults None.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage Enable the MOTD prompt, then optionally specify a prompt message. When a user logs into the MX using the CLI, the configured MOTD banner is displayed, followed by the MOTD prompt message (if one is specified). In response, the user has the option of entering **y** to proceed or any other key to terminate the connection.

Examples To enable the prompt for the MOTD banner, type the following command:

```
MX# set banner acknowledge enable
success: change accepted.
```

To set as the text to be displayed following the MOTD banner, type the following command:

```
MX# set banner acknowledge message 'Do you agree?'
success: change accepted.
```

After these commands are entered, when the user logs on, the MOTD banner is displayed, followed by the text If the user enters , then the login proceeds. If not, then the user is disconnected.

Quotation marks can be used in the message if they are enclosed by delimiting characters. For example, to set the text (including the quotation marks) as the text to be displayed following the MOTD banner, type the following command:

```
MX# set banner acknowledge message '"Do you agree?"'
success: change accepted.
```

See Also

- **set banner motd** on page 4-25
- **clear banner motd** on page 4-19
- **show banner motd** on page 4-35

set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the MX.

Syntax **set banner motd "***text***"**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage

set length

Defines the number of lines of CLI output to display between paging prompts. MSS displays the set number of lines and waits for you to press any key to display another set, or type **q** to quit the display.

Syntax **set length** *screenlength*

screenlength Number of lines of text to display between paging prompts. You can specify 0 and from 10 to 512. The 0 value disables the paging prompt action entirely.

Defaults MSS displays 24 lines by default.

Access All.

History

Version 1.0	Command introduced.
Version 6.0	Minimum screen length set to 10 lines.
Version 7.0	Changed variable from to

Usage Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

Examples To set the number of lines displayed to 100, type the following command:

```
MX# set length 100
success: screen length for this session set to 100
```

set license

Installs an upgrade license key on an MX-200, MX-216, or MX-400.

The MX-200 and MX-216 can boot and manage up to 32 MPs by default. You can increase the MP support to 64, 96, or 128 MPs, by installing one or more activation keys. You can install a 32-MP upgrade, 64-MP upgrade, or 96-MP upgrade. If you have already installed a 32-MP or 64-MP upgrade, you can still install additional upgrades.

The MX-400 can boot and manage up to 40 MPs by default. You can increase the MP support to 80 MPs or 120 MPs, by installing one or two activation keys. You can install a 40-MP upgrade or an 80-MP upgrade. If you have already installed a 40-MP upgrade, you can install an additional 40-MP upgrade.

Syntax **set license** *activation-key*

activation-key

Defaults None.

Access Enabled.

History

Usage

set system contact

Stores a contact name for the MX.

Syntax **set system contact** *string*

string Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

To view the system contact string, type the **show system** command.

Examples The following command sets the system contact information to :

```
MX# set system contact tamara@example.com
success: change accepted.
```

See Also

- **clear system** on page 4-21
- **set system location** on page 4-34
- **set system name** on page 4-35
- **show system** on page 4-40

set system countrycode

Defines the country-specific IEEE 802.11 regulations to enforce on the MX.

Syntax **set system countrycode** *code*

code Two-letter code for the country of operation for the MX. You can specify one of the codes listed in **Table 4– 1**.

Algeria	**DZ**
Argentina	**AR**
Anguilla	**AI**
Australia	**AU**
Austria	**AT**
Bosnia and Herzegovia	BA
Belgium	**BE**
Bulgaria	**BG**
Bahrain	**BH**
Bolivia	**BO**
Botswana	**BW**

Kenya	KE
St. Kitts and Nevis	KN
Kuwait	KW
Cayman Islands	KY
Latvia	LV
Lebanon	LB
Liechtenstein	LI
Lithuania	LT
St. Lucia	LC
Liechtenstein	**LI**
Luxembourg	**LU**
Macedonia, Former Yuogoslave Republic of	MK
Malaysia	**MY**
Malta	MT
Mauritius	MU
Mexico	**MX**
Monserrat	MS
Morocco	MA
Namibia	NA
Netherlands	**NL**
New Zealand	**NZ**
Nigeria	NG
Norway	**NO**
Oman	OM
Pakistan	PK
Panama	PA
Paraguay	PY
Peru	PE
Philippines	PH
Poland	**PL**
Portugal	**PT**
Puerto Rico	PR
Qatar	QA
Romania	RO
Russia	RU
Saudi Arabia	**SA**
Serbia	CS

Singapore	**SG**
Slovakia	**SK**
Slovenia	**SI**
South Africa	**ZA**
South Korea	**KR**
Spain	**ES**
Sri Lanka	LK
Sweden	**SE**
Switzerland	**CH**
Taiwan	**TW**
Tanzania	TZ
Thailand	**TH**
East Timor	TP
Trinidad and Togo	TT
Tunisia	TN
Turkey	TR
Ukraine	UA
United Arab Emirates	**AE**
United Kingdom	**GB**
United States	**US**
Uruguay	UY
Venezuela	VE
Vietnam	VN
St. Vincent and the Grenadines	VC
US Virgin Islands	VI
Zambia	ZM
Zimbabwe	ZW

Defaults The factory default country code is .

Access Enabled.

History

Version 1.0	Command introduced
Version 1.1	New country codes added: **AE**, **AU**, **BR**, **CN**, **CZ**, **ES**, **GR**, **HK**, **HU**, **KR**, **IL**, **IN**, **LI**, **MX**, **MY**, **NZ**, **PL**, **SA**, **SG**, **SI**, **SK**, **TH**, **TW**, **ZA**
Version 6.2	New country codes added: **BH, BO, BW, CL, CO CR, CI, HR, CY, DM, DO, EC, SV, EG, EE, GD, GT, HN, ID, JM, JO, KZ, KE, KN, KW, KY, LV, LB, LI, LT, LC, MU, MS, MA, NA, NG, OM, PK, PA, PY, PE, PH, PR, RO, RU, CS, LK, TZ, TT, TN, TR, UA, UY, VE, VN, VC, ZM,** and **ZW**.

Usage You must set the system county code to a valid value before using any **set ap** commands to configure a Mobility Point (MP).

Examples To set the country code to Canada, type the following command:

set system ip-address

Sets the system IP address so that it can be used by various services in the MX.

Syntax **set system ip-address** *ip-addr*

Defaults None.

set system name

Changes the name of the MX from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

Syntax **set system name** *string*

Defaults By default, the system name and command prompt have the same value. The factory default for both is *-nnnnnn*, where is the model number and *nnnnnn* is the last 6 digits of the 12-digit system MAC address.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Entering **set system name** with no string resets the system name to the factory default.

To view the system name string, type the **show system** command.

Examples The following example sets the system name to a name that identifies the MX switch:

```
MX# set system name MX-bldg3
success: change accepted.
MX-bldg3#
```

See Also

- **clear system** on page 4-21
- **set prompt** on page 4-28
- **set system contact** on page 4-29
- **set system location** on page 4-34
- **show system** on page 4-40

Syntax **show license keys**

Defaults None.

Access All.

History

Version 1.0	Command introduced.
Version 2.0	Current session count and Last sent alert time fields removed.
Version 3.1	Command readded as **show licenses**, with new output.
Version 7.0	Command changed to **show license keys** with new output.

Usage This command applies only to the MX-200, MX-216, and MX-400.

Examples To view license keys, type the following command:

```
MX# show license keys
Serial Number    : 0321300013

40 access points are supported

Additional Features:

        Feature Description               Installed  Active
        ------------------------------------------------

Installed License Authorization Keys
```

See Also **set license** on page 4-27

show load

Changes to the **show load** command allows you to obtain instantaneous CPU and memory load information in a more useful format. In addition, more information is provided that may assist with troubleshooting the MX on the network.

The following information is displayed:

- System CPU load

  Summary data displayed:

  - Last second (also called instant load)
  - Last minute
  - Last 5 minutes
  - Last hour
  - Last day
  - Last three days

  Historical values drawn as a graph, showing peaks and averages:

  - Last minute
  - Last hour
  - Last three days
- System memory load

  Summary data displayed:

  - Last second (also called instant load)
  - Last minute
  - Last 5 minutes
  - Last hour
  - Last day
  - Last three days

  Historical values drawn as a graph, showing peaks and averages:

  - Last minute
  - Last hour
  - Last three days

Syntax **show load**

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.1.

Version 4.1	Command introduced.
Version 6.2	Enhancements to output format.

Usage To display the CPU load recorded from the time the MX was booted, as well as from the previous time the **show load** command was run, type the following command:

```
MXR2_desk# show load cpu
Period         Usage
--------------------
Last second:    2%
Last minute:    2%
Last 5 minutes: 2%
Last hour:      2%
Last day:       1%
Last 3 days:    33141%

MXR2_desk# show load cpu history
                                                                |100
                                                                |90
                                                                |80
                                                                |70
                                                                |60
                                                                |50
                                                                |40
                                                                |30
                                                                |20
   ^  ^             ^   ^^      ^  ^   ^       ^  ^       ^|10
  ************************************************************|<5
  6----5----5----4----4----3----3----2----2----1----1----5----0---
  0    5    0    5    0    5    0    5    0    5    0         |
               CPU load history for the past hour
        * = average CPU load (%)    ^ = peak CPU load (%)
MXR2_desk# show load memory history
                                                                  |128
                                                                  |112
                                                                  |96
                                                                  |80
                                                                  |64
                                                                  |48
     ************************************************************|32
     ************************************************************|16
     ************************************************************|<8
     6----5----5----4----4----3----3----2----2----1----1----5----0---
```

```
          0    5    0    5    0    5    0    5    0    5    0        |
                        Memory utilization history for the past hour
      * = average utilization (MBytes)    ^ = peak utilization (MBytes)
```

The overall field shows the CPU load as a percentage from the time the MX was booted. The delta field shows CPU load as a percentage from the last time the **show load** command was entered.

See Also **show system** on page 4-40

show system

Displays system information.

Syntax **show system**

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 2.0	System Description field added
Version 3.0	System Description field removed
Version 4.0	License field removed. To display license information, use the **show license** command.
Version 7.0	Total Power over Ethernet changed to Total PoE draw (W).

Examples To show system information, type the following command:

```
MX# show system
================================================================================
 Product Name:       MX
 System Name:        MX-bldg3
 System Countrycode: US
 System Location:    first-floor-bldg3
 System Contact:     tamara@example.com
 System IP:          192.168.12.7
 System idle timeout:3600
 System MAC:         00:0B:0E:00:04:30
================================================================================
 Boot Time:          2003-11-07 15:45:49
 Uptime:                 13 days 04:29:10
================================================================================
 Fan status:  fan1 OK fan2 OK fan3 OK
 Temperature: temp1 ok  temp2 ok  temp3 ok
 PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
 Memory:      97.04/744.03 (13%)
 Total PoE Draw (W): 29.000
================================================================================
```

Table 4– 2 describes the fields of **show system** output.

Product Name	MX model number.
System Name	System name (factory default, or optionally configured with **set system name**).
System Countrycode	Country-specific 802.11 code required for MP operation (configured with **set system countrycode**).
System Location	Record of MX physical location (optionally configured with **set system location**).
System Contact	Contact information about the system administrator or another person to contact about the system (optionally configured with **set system contact**).
System IP	Common interface, source, and default IP address for the MX, in dotted decimal notation (configured with **set system ip-address**).
System idle timeout	Number of seconds MSS allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the **set system idle-timeout** command.)
System MAC	MX media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format.
Boot Time	Date and time of the last system reboot.
Uptime	Number of days, hours, minutes, and seconds that the MX has been operating since its last restart.
Fan status	Operating status of the three MX cooling fans: ❑ OK—Fan is operating. ❑ Failed—Fan is not operating. MSS sends an alert to the system log every 5 minutes until this condition is corrected. Fan 1 is located nearest the front of the chassis, and fan 3 is located nearest the back.
Temperature	Status of temperature sensors at three locations in the MX switch: ❑ ok—Temperature is within the accis 6(an is c 42t).4(i9 a(A)1.(in)-4.g(n)2.e(s o0°(e)-)-1.C(t t50°(e)-)-1.C(4

See Also

- **clear system** on page 4-21
- **set system contact** on page 4-29
- **set system countrycode** on page 4-29
- **set system idle-timeout** on page 4-33
- **set system ip-address** on page 4-34
- **set system location** on page 4-34

- **set system name** on page 4-35

show tech-support

Provides an in-depth snapshot of the status of the MX, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

Syntax **show tech-support** [**file** [*subdirname/*]*filename*]

[*subdirname/*]*filename*	Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Enter this command before calling the Trapeze Networks Technical Assistance Center (TAC). See **"Contacting the Technical Assistance Center" on page 1–1** for more information.

See Also

- **show boot** on page 21-497
- **show config** on page 21-499
- **show license** on page 4-35
- **show system** on page 4-40
- **show version** on page 21-500

clear ap

Removes a Distributed MP.

When you clear a Distributed MP, MSS ends user sessions that are using the MP.

clear ap {*apnum* | **all**}

apnum	Number of the MP(s) to remove.
all	Clear all MPs.

None.

Enabled.

History

MSS Version 2.0	Command introduced.
MSS Version 6.0	Command changed from **dap** to **ap**.

The following command clears MP 1:

```
MX# clear ap 1
This will clear specified AP devices. Would you like to continue? (y/n) [n]y
```

- **set ap** on page 5-51
- **set port type ap** on page 5-58

clear port counters

Clears port statistics counters and resets them to 0.

Syntax **clear port counters**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command clears all port statistics counters and resets them to 0:

```
MX# clear port counters
success: cleared port counters
```

See Also

- **monitor port counters** on page 5-47
- **show port counters** on page 5-60

clear port-group

Removes a port group.

Syntax **clear port-group name** *name*

name *name* Name of the port group.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command clears port group :

```
MX# clear port-group name server1
success: change accepted.
```

See Also

- **set port-group** on page 5-53
- **show port-group** on page 5-61

clear port media-type

Disables the copper interface and reenables the fiber interface on an MX-400 gigabit Ethernet port.

Syntax **clear port media-type name**

name List of physical ports. MSS disables the copper interface and reenables the fiber interface on all the specified ports.

Defaults The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Access Enabled.

History

MSS Version 4.0	Command introduced.
MSS Version 7.0	*port-list* changed to literal value of **name**.

Usage This command applies only to the MX-400. This command does not affect a link that is already active on the port.

Examples The following command disables the copper interface and reenables the fiber interface on port 2:

```
MX-400# clear port media-type name
```

See Also

- **set port media-type** on page 5-54
- **show port media-type** on page 5-61

clear port mirror

Removes a port mirroring configuration.

Syntax **clear port mirror**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Use this command to change a port back to a network port. All configuration settings specific to the port type are removed. For example, if you clear an MP port, all MP-specific settings are removed. **Table 5– 3** lists the default network port settings that MSS applies when you clear a port type.

VLAN membership	None. **Note:** Although the command changes a port to a network port, the command does not place the port in any VLAN. To use the port in a VLAN, you must add the port to the VLAN.
Spanning Tree Protocol (STP)	Based on the VLAN(s) you add the port to.
802.1X	No authorization.
Port groups	None.
Internet Group Management Protocol (IGMP) snooping	Enabled as port is added to VLANs.
Access point and radio parameters	Not applicable
Maximum user sessions	Not applicable

Examples The following command clears port 5:

```
MX# clear port type 5
This may disrupt currently authenticated users. Are you sure? (y/n) [n]y
success: change accepted.
```

See Also

- **set port type ap** on page 5-58
- **set port type wired-auth** on page 5-58

monitor port counters

Displays and continually updates port statistics.

Syntax **monitor port counters** [**octets** | **packets** | **receive-errors** | **transmit-errors** | **collisions** | **receive-etherstats** | **transmit-etherstats**]

octets	Displays octet statistics first.
packets	Displays packet statistics first.
receive-errors	Displays errors in received packets first.
transmit-errors	Displays errors in transmitted packets first.
collisions	Displays collision statistics first.
receive-etherstats	Displays Ethernet statistics for received packets first.
transmit-etherstats	Displays Ethernet statistics for transmitted packets first.

Defaults All types of statistics are displayed for all ports. MSS refreshes the statistics every 5 seconds, and the interval cannot be configured. Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

Access All.

History Introduced in MSS Version 1.0.

Table 5– 5 describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.

Displayed for All Options	Port	Displays the port statistics.
	Status	Port status. The status can be Up or Down.
octets	Rx Octets	Total number of octets received by the port. This number includes octets received in frames that contained errors.
	Tx Octets	Total number of octets received. This number includes octets received in frames that contained errors.
packets	Rx Unicast	Number of unicast packets received. This number does not include packets that contain errors.
	Rx NonUnicast	Number of broadcast and multicast packets received. This number does not include packets that contain errors.
	Tx Unicast	Number of unicast packets transmitted. This number does not include packets that contain errors.
	Tx NonUnicast	Number of broadcast and multicast packets transmitted. This number does not include packets that contain errors.
receive-errors	Rx Crc	Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors.
	Rx Error	Total number of frames received in which the Physical layer (PHY) detected an error.
	Rx Short	Number of frames received by the port that were fewer than 64 bytes long.
	Rx Overrun	Number of frames received by

receive-etherstats	Rx 64	Number of packets received that were 64 bytes long.
	Rx 127	Number of packets received that were from 65 through 127 bytes long.
	Rx 255	Number of packets received that were from 128 through 255 bytes long.
	Rx 511	Number of packets received that were from 256 through 511 bytes long.
	Rx 1023	Number of packets received that were from 512 through 1023 bytes long.
	Rx 1518	Number of packets received that were from 1024 through 1518 bytes long.
transmit-etherstats		

See Also **show port counters** on page 5-60

reset port

Resets a port by toggling the link state and Power over Ethernet (PoE) state.

Syntax **reset port** *port-list*

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage The **reset** command disables the port link and PoE (if applicable) for at least 1 second, then reenables them. This behavior is useful for forcing an MP that is connected to two MX switches to reboot over the link to the other MX.

Examples The following command resets port 5:

```
MX# reset port 5
```

See Also **set port** on page 5-52

set ap

Configures an MP, either directly connected to the MX or indirectly connected through an intermediate Layer 2 or Layer 3 network.

Syntax **set ap** *apnum* **serial-id** *serial-ID*
model {**2330** | **2330A** | **AP2750** | **AP3750 | AP3850 | AP3950 |mp-371** | **mp-372** | **mp-372-JP | mp-372A | mp-422 | mp-422A | mp-422F|mp-432** | **mp-620 | mp-620A | mp-371**}
[**radiotype** {**11a** | **11b**| **11g | 11na | 11ng**}]

Defaults The default vales are the same as the defaults for the **set port type ap** command.

Access Enabled.

History

Version 3.0 New values for

Examples The following command configures MP 1 for MP model MP-372 with serial-ID 0322199999:

```
MX# set ap 1 serial-id 0322199999 model mp-372
success: change accepted.
```

The following command removes MP 1:

```
MX# clear ap 1
This will clear specified AP devices. Would you like to continue? (y/n) [n]y
```

See Also

- **clear ap** on page 5-44
- **clear port type** on page 5-46
- **set port type ap** on page 5-58
- **set system countrycode** on page 4-29

set port

Administratively disables or reenables a port.

Syntax **set port** {**enable** | **disable**} *port-list*

Defaults All ports are enabled.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Examples The following command disables port 16:

set port media-type

Disables the fiber interface and enables the copper interface on an MX-400 gigabit Ethernet port.

Syntax **set port media-type name** *port-name*

Defaults The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage This command applies only to the MX-400.

set port name

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

Syntax **set port** *port* **name** *name*

port	Number of a physical port. You can specify only one port.
name *name*	Alphanumeric string of up to 16 characters, with no spaces.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage To simplify configuration and avoid confusion between the number of a port and its name, it is recommended that you do not use numbers as port names.

Examples The following command sets the name of port 17 to :

```
MX# set port 17 name adminpool
success: change accepted.
```

See Also

- **clear port name** on page 5-46
- **show port status** on page 5-64

set port negotiation

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

Syntax **set port negotiation** *port-list* {**enable** | **disable**}

port-list	List of physical ports. MSS disables or reenables autonegotiation on all the specified ports.
enable	Enables autonegotiation on the specified ports.
disable	Disables autonegotiation on the specified ports.

Defaults Autonegotiation is enabled on all Ethernet ports by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage The gigabit Ethernet ports operate at 1000 Mbps only. They do not change speed to match 10-Mbps or 100-Mbps links.

MX-8, MX-200, and MX-216 10/100 Ethernet ports support half-duplex and full-duplex operation.

MX-20 10/100 Ethernet ports do not support half-duplex operation. As a result, there are restrictions when MX-20 10/100 Ethernet ports are interoperating with other vendor devices. For a link to occur, the autonegotiation settings on an MX-20 port and the device at the other end of the link must be the same. In addition, the other device must support full-duplex operation. When autonegotiation is enabled on an MX-20 port, the port advertises support for full-duplex mode only. **Table 5– 6** lists the supported configurations.

	100 Mbps full-duplex	Not supported	Not supported
	Not supported	10 Mbps full-duplex	Not supported
	Not supported	Not supported	Not supported
	Not supported	Not supported	Not supported
	Not supported	Not supported	100 Mbps full-duplex

It is recommended that you do not configure the mode of an MX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can cause slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an MX port with this configuration can cause forwarding on the link to stop.

Examples The following command disables autonegotiation on ports 3, 8, and 16 through 18:

```
MX# set port negotiation 3,8,16-18 disable
```

The following command enables autonegotiation on port 21:

```
MX# set port negotiation 21 enable
```

set port poe

Enables or disables Power over Ethernet (PoE) on ports connected to MPs.

When you set the port type for MP use, you can enable PoE on the port. Use the MX PoE to power Trapeze Networks MP access points only. If you enable PoE on ports connected to other devices, damage can result.

Syntax **set port poe** *port-list* **enable** | **disable**

port-list	List of physical ports. MSS disables or reenables PoE on all the specified ports.
enable	Enables PoE on the specified ports.
disable	Disables PoE on the specified ports.

Defaults PoE is disabled on network and wired authentication ports. The state on MP ports depends on whether you enabled or disabled PoE when setting the port type. See **set port type ap** on page 5-58.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage This command does not apply to any gigabit Ethernet ports or to ports 7 and 8 on the MX-8 switch, port 19 on the MX-216, or port 3 on the MX-200.

Examples The following command disables PoE on ports 7 and 9, which are connected to an MP:

```
MX# set port poe 7,9 disable
If you are enabling power on these ports, they must be connected only to approved PoE devices
with the correct wiring. Do you wish to continue? (y/n) [n]y
```

The following command enables PoE on ports 7 and 9:

```
MX# set port poe 7,9 enable
If you are enabling power on these ports, they must be connected only to approved PoE devices
with the correct wiring. Do you wish to continue? (y/n) [n]y
```

See Also

- **set port type ap** on page 5-58
- **set port type wired-auth** on page 5-58

set port preference

Deprecated in MSS Version 4.0 Use the **set port media-type** command.

set port speed

Changes the speed of a port.

Syntax **set port speed** *port-list* {**10** | **100** | **1000** | **auto**}

port-list	List of physical ports. MSS sets the port speed on all the specified ports.
10	Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex.
100	Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex.
1000	Sets the port speed of a gigabit Ethernet port to 1000 Mbps and sets the operating mode to full-duplex.
10000	Sets the port speed of a gigabit Ethernet port to 10000 Mbps and sets the operating mode to full-duplex.
auto	Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly.

Defaults All ports are set to **auto**.

Access Enabled.

History Introduced in MSS Version 1.0.

Version 1.0	Command introduced.
Version 7.0	Added 10000 as a port speed.

Usage It is recommended that you do not configure the mode of an MX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an MX port in such a configuration can cause forwarding on the link to stop.

Do not set the port speed of a gigabit port to **auto**. Although the CLI allows this setting, it is invalid. If you set the port speed of a gigabit port to **auto**, the link will stop working.

Examples The following command sets the port speed on ports 1, 7 through 11, and 14 to 10 Mbps and sets the operating mode to full-duplex:

```
MX# set port speed 1,7-11,14 10
```

set port trap

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

Syntax **set port trap** *port-list* {**enable** | **disable**}

Defaults SNMP linkup and linkdown traps are disabled by default.

Access Enabled.

History Introduced in MSS Version 1.1.

Usage The **set port trap** command overrides the global setting of the **set snmp trap** command.

The **set port type** command does not affect the global trap information displayed by the **show snmp configuration** command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the **show snmp configuration** command still indicates that the

Syntax **set port type wired-auth** *port-list* [**tag** *tag-list*] [**max-sessions** *num*] [**auth-fall-thru** {**last-resort** | **none** | **web-portal**}]

Defaults The default tag-list is null (no tag values). The default number of sessions is 1. The default fallthru authentication type is **none**.

Access Enabled.

History

Usage You cannot set a port type if the port is a member of a port VLAN. To remove a port from a

- **monitor port counters** on page 5-47

show port-group

Displays port group information.

Syntax **show port-group** [**name** *group-name*]

name *group-name*	Displays information for the specified port group.

Defaults None.

Access All.

History

Version 1.0	Command introduced.
Version 4.2	Option **all** removed for simplicity. You can display information for all groups by entering the command without specifying a group name.

Examples The following command displays the configuration of port group :

```
MX# show port-group name server2
Port group: server2 is up
        Ports:  15, 17
```

Table 5– 8 describes the fields in the **show port-group** output.

Port group	Name and state (enabled or disabled) of the port group.
Ports	Ports contained in the port group.

See Also

- **clear port-group** on page 5-44
- **set port-group** on page 5-53

show port media-type

Displays the enabled interface types on an MX-400 switch's gigabit Ethernet ports.

Syntax **show port media-type** [*port-list*]

port-list	List of physical ports. MSS displays the enabled interface types for all specified ports.

Defaults None.

Access All.

History Introduced in MSS Version 4.0.

Usage This command applies only to the MX-400.

Examples The following command displays the enabled interface types on all four ports of an MX-400:

```
MX-400# show port media-type
Port  Media Type
============================================================
   1  GBIC
   2  RJ45
   3  GBIC
   4  GBIC
```

Table 5– 9 describes the fields in this display.

See Also

- **clear port media-type** on page 5-45
- **set port media-type** on page 5-54

show port mirror

Displays the port mirroring configuration.

Syntax **show port mirror**

Defaults None.

Access Enabled.

History

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command displays PoE information for all ports on a 22-port MX:

```
MX# show port poe
                     Link     Port   PoE       PoE
Port  Name           Status   Type   config    Draw
================================================================================
   1  1              up       -      disabled  off
   2  2              down     -      disabled  off
   3  3              down     -      disabled  off
   4  4              down     -      disabled  off
   5  5              down     -      disabled  off
   6  6              down     -      disabled  off
   7  7              down     -      disabled  off
   8  8              down     -      disabled  off
   9  9              up       MP     enabled   1.44
  10  10             up       -      disabled  off
  11  11             down     -      disabled  off
  12  12             down     -      disabled  off
  13  13             down     -      disabled  off
  14  14             down     -      disabled  off
  15  15             down     -      disabled  off
  16  16             down     -      disabled  off
  17  17             down     -      disabled  off
  18  18             down     -      disabled  off
  19  19             down     -      disabled  off
  20  20             down     -      disabled  off
  21  21             down     -      disabled  invalid
  22  22             down     -      disabled  invalid
```

Table 5– 10 describes the fields in this display.

Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.
Link status	Link status of the port: ❑ up—The port is connected. ❑ down—The port is not connected.
Port type	Port type: ❑ MP—The port is an MP access port. ❑ - (The port is not an MP access port.)
PoE config	PoE state: ❑ enabled ❑ disabled
PoE Draw	Power draw on the port, in watts. For 10/100 Ethernet ports on which PoE is disabled, this field displays . For gigabit Ethernet ports, this field displays , because PoE is not supported on gigabit Ethernet ports. The value indicates a PoE problem such as a short in the cable.

See Also **set port poe** on page 5-56

show port preference

Deprecated in MSS Version 4.0 Use the **show port media-type** command.

show port status

Displays configuration and status inc33y.rendDisplays configuration and st

Oper	Operational status of the port: ❑ up—The port is operational. ❑ down—The port is not operational.
Config	Port speed configured on the port: ❑ 10—10 Mbps. ❑ 100—100 Mbps. ❑ 1000—1000 Mbps. ❑ auto—The port sets its own speed.
Actual	Speed and operating mode in effect on the port.
Type	Port type: ❑ ap—MP port ❑ network—Network port ❑ wa—Wired authentication port
Media	Link type: ❑ 10/100BaseTX—10/100BASE-T. ❑ GBIC—1000BASE-SX or 1000BASE-LX GBIC. ❑ 1000BaseT—1000BASE-T. ❑ No connector—GBIC slot is empty.

See Also

- **clear port type** on page 5-46
- **set port** on page 5-52
- **set port name** on page 5-55
- **set port negotiation** on page 5-55
- **set port speed** on page 5-57
- **set port type ap** on page 5-58
- **set port type wired-auth** on page 5-58

Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients roaming within a mobility domain. This chapter presents VLAN commands alphabetically. Use the following table to locate commands in this chapter based on use.

Creation	**set vlan name** on page 6-73
Ports	**set vlan port** on page 6-74
	clear vlan on page 6-70
	show vlan config on page 6-81
Roaming and Tunnels	**show roaming station** on page 6-78
	show roaming vlan on page 6-79
	show tunnel on page 6-81
Restriction of Client Layer 2 Forwarding	**set security l2-restrict** on page 6-72
	show security l2-restrict on page 6-80
	clear security l2-restrict on page 6-68
	clear security l2-restrict counters on page 6-69
Tunnel Affinity	**set vlan tunnel-affinity** on page 6-75
FDB Entries	**set fdb** on page 6-71
	show fdb on page 6-76
	show fdb count on page 6-78
	clear fdb on page 6-67
FDB Aging Timeout	**set fdb agingtime** on page 6-72
	show fdb agingtime on page 6-77
VLAN Profiles for MP local switching	**set vlan-profile** on page 6-75
	show vlan-profile on page 6-83
	clear vlan-profile on page 6-71

clear fdb

Deletes an entry from the forwarding database (FDB).

Syntax **clear fdb** {*address-mode* **static |permanent | system**} [*mac-addr*] [**dynamic | port** *port-list* | [**vlan** *vlan-id*]

address-mode **perm**	Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
static	Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.

Defaults If you do not specify a list of MAC addresses or **all**, all addresses are removed.

Access

clear vlan

Removes physical or virtual ports from

clear vlan-profile

Removes a VLAN profile or individual entries from a VLAN profile.

Syntax **clear vlan-profile** *profile-name* [**vlan** *vlan-name*]

ss1 60

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You cannot add a multicast or broadcast address as a permanent or static FDB entry.

Examples The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 3 and 5 in VLAN :

```
MX# set fdb perm 00:11:22:aa:bb:cc port 3,5 vlan blue
success: change accepted.
```

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the VLAN:

```
MX# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

See Also

- **clear fdb** on page 6-67
- **show fdb** on page 6-76

set fdb agingtime

Changes the aging timeout period for dynamic entries in the forwarding database.

Syntax **set fdb agingtime** *vlan-id* **age** *seconds*

Defaults The aging timeout period is 300 seconds (5 minutes).

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command changes the aging timeout period to 600 seconds for

communicate directly to each other. To communicate with another client, the client must use one of the specified default routers.

Syntax **set security l2-restrict vlan** *vlan-id* [**mode** {**enable** | **disable**}] [**permit-mac** *mac-addr* [*mac-addr*]]

Defaults Layer 2 restriction is disabled by default.

Access Enabled.

History Introduced in MSS Version 4.1.

Usage You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the **clear security l2-restrict** command to remove it, anJ/846eYou ca 7n(031 nD.0031 7n Tc-.0011 Tw[(c8 -165municate with a6 1 Tw[((set(e

You cannot use a number as the first character in the VLAN name. It is recommended that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names and .

VLAN names are case-sensitive for RADIUS authorization when a client roams to an MX. If the switch is not configured with the VLAN of the client, but is configured with a VLAN with the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN but the MX to which the client roams has VLAN instead, RADIUS authorization fails.

Examples The following command assigns the name to VLAN 3:

```
MX# set vlan 3 name marigold
success: change accepted.
```

See Also **set vlan port** on page 6-74

set vlan port

Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

Syntax **set vlan** *vlan-id* **port** *port-list* [**tag** *tag-value*]

vlan-id	VLAN name or number.
port *port-list*	List of physical ports.
tag *tag-value*	Tag value that identifies a virtual port. You can specify a value from 1 through 4093.

Defaults By default, no ports are members of any VLANs. An MX cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You can combine this command with the **set port name** command to assign the name and add the ports at the same time.

If you do not specify a tag value, the MX sends untagged frames for the VLAN. If you do specify a tag value, the MX sends tagged frames only for the VLAN.

If you do specify a tag value, it is recommended to use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same but it can be required by devices from other vendors.

Examples The following command assigns the name to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
MX# set vlan 11 name beige port 1-3
success: change accepted.
```

The following command adds port 16 to VLAN and assigns tag value 86 to the port:

```
MX# set vlan beige port 16 tag 86
success: change accepted.
```

See Also

- **clear vlan** on page 6-70
- **set vlan name** on page 6-73
- **show vlan config** on page 6-81

set vlan tunnel-affinity

Changes an MX preferences within a mobility domain for tunneling user traffic for a VLAN. When a user roams to an MX that is not a member of the user's VLAN, the MX can forward the user traffic by tunneling to another MX that is a member of the VLAN.

Syntax **set vlan** *vlan-id* **tunnel-affinity** *num*

vlan-id	VLAN name or number.
num	Preference of this MX for forwarding user traffic for the VLAN. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults Each VLAN on an MX network ports has an affinity value of 5 by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Increasing a MX affinity value increases the preferability of the MX for forwarding user traffic for the VLAN.

If more than one MX has the highest affinity value, MSS randomly selects one of the switches for the tunnel.

Examples The following command changes the VLAN affinity for VLAN to 10:

```
MX# set vlan beige tunnel-affinity 10
success: change accepted.
```

See Also

- **show roaming vlan** on page 6-79
- **show vlan config** on page 6-81

set vlan-profile

Configures entries in a VLAN profile that can be applied to an MP for local switching.

Syntax **set vlan-profile** *profile-name* **vlan** *vlan-name*
[**tag** *tag-value*]

profile-name	VLAN profile name.
vlan-name	Name of a VLAN.
tag-value	Optional tag value associated with the VLAN. When this value is set, it is used as the 802.1Q tag for the VLAN.

Defaults If local switching is enabled on an MP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named that is untagged.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to an MP, traffic for the VLANs specified in the VLAN profile is locally switched by the MP instead of being tunneled back to an MX.

You enter a separate **set vlan-profile** command for each VLAN you want to add to the VLAN profile. A VLAN profile can contain up to 128 entries.

Examples The following command adds an entry for VLAN to VLAN profile :

```
MX# set vlan-profile locals vlan red
success: change accepted.
```

See Also

- **set ap local-switching vlan-profile** on page 12-242
- **clear vlan-profile** on page 6-71
- **show vlan-profile** on page 6-83

show fdb

Displays entries in the forwarding database.

Syntax **show fdb** [*mac-addr-glob* [**vlan** *vlan-id*]]

show fdb {**perm** | **static** | **dynamic** | **system** | **all**} [**port** *port-list* | **vlan** *vlan-id*]

mac-addr-glob	A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*) to specify a set of MAC addresses. (For details, see **"MAC Address Globs" on page 2–7**.)
vlan *vlan-id*	Name or number of a VLAN to display entries.
perm	Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
dynamic	Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
system	Displays system entries. A system entry is added by MSS. For example, the authentication protocols can add entries for wired and wireless authentication users.
all	Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN.
port *port-list*	Destination port(s) for which to display entries.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Usage To display the entire forwarding database, enter the **show fdb** command without options. To display only a portion of the database, use optional parameters to specify the types of entries to display.

Examples The following command displays all entries in the forwarding database:

```
MX# show fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      aa:bb:cc:dd:ee:ff      *       3                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 3
```

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
MX# show fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ----------------- -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 2
```

Table 6– 12 describes the fields in the **show fdb** output.

VLAN	VLAN number.
TAG	VLAN tag value. If the interface is untagged, the TAG field is blank.
Dest MAC/Route Des	MAC address of the forwarding entry destination.
CoS	Type of entry. The entry types are explained in the first row of the command output. **Note:** This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.
Destination Ports	MX port associated with the entry. A MX sends traffic to the destination MAC address through this port.
Protocol Type	Layer 3 protocol address types that can be mapped to this entry.
Total Matching FDB Entries Displayed	Number of entries displayed by the command.

See Also

- **clear fdb** on page 6-67
- **set fdb** on page 6-71

show fdb agingtime

Displays the aging timeout period for forwarding database entries.

Syntax **show fdb agingtime** [**vlan** *vlan-id*]

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command displays the aging timeout period for all VLANs:

```
MX# show fdb agingtime
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec
```

Because the forwarding database aging timeout period can be configured on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.

See Also **set fdb agingtime** on page 6-72

show fdb count

Lists the number of entries in the forwarding database.

Syntax **show fdb count** {**perm** | **static** | **dynamic**} [**vlan** *vlan-id*]

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command lists the number of dynamic entries that the forwarding database contai[(Sy)N–2d9in|

Table 6– 13 describes the fields in the display.

User Name	Name of the user. This is the name used for authentication. The name resides in a RADIUS server database or the local user database on an MX.
Station Address	IP address of the user device.
VLAN	Name of the VLAN that the RADIUS server or MX local user database assigned the user.
State	State of the session: ❑ Setup—Station is attempting to roam to this MX. This switch has asked the MX from which the station is roaming for the station session information and is waiting for a reply. ❑ Up—MSS has established a tunnel between the MX switches and the station has successfully roamed to this MX over the tunnel. ❑ Chck—This MX is in the process of accepting a reassociation request from the roaming peer MX for a station currently roaming to the peer switch. ❑ TChck—This MX is in the process of accepting a reassociation request from the roaming peer MX for a station currently roaming to this switch. ❑ WInd—This MX is waiting for network congestion to clear before sending the roaming indication to the roaming peer MX. ❑ WResp—This MX is waiting for network congestion to clear before sending the roaming response to the roaming peer MX.

See Also **show roaming vlan** on page 6-79

show roaming vlan

Shows all VLANs in the mobility domain, the MX switches servicing the VLANs, and the tunnel affinity values configured on each MX for the VLANs.

Syntax **show roaming vlan**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command shows the current roaming VLANs:

```
MX# show roaming vlan
VLAN             Switch IP Address Affinity
---------------- ---------------- --------
vlan-cs          192.168.14.2           5
vlan-eng         192.168.14.4           5
vlan-fin         192.168.14.2           5
vlan-it          192.168.14.4           5
vlan-it          192.168.14.2           5
vlan-pm          192.168.14.2           5
vlan-sm          192.168.14.2           5
vlan-tp          192.168.14.4           5
vlan-tp          192.168.14.2           5
```

Table 6– 14 describes the fields in the display.

show vlan-profile

Displays the contents of the VLAN profiles configured on the MX. A VLAN profile lists the VLANs that traffic is locally switched by MPs with the VLAN profile.

Syntax **show vlan-profile** [*profile-name*]

profile-name VLAN profile name

Defaults If a *profile-name* is not specified, the contents of all VLAN profiles configured on the MX switch are displayed.

Access All.

History Introduced in MSS Version 6.0.

Examples The following command displays the contents of VLAN profile :

```
MX# show vlan-profile locals
vlan-profile: locals
AP list: 1,2,3
  Vlan Name            Tag
  ---------            ---
  blue                 none
  red                  45

  ap numbers: 67
```

Table 6– 18 describes the fields in the **show vlan-profile** output.

vlan-profile	Name of the VLAN profile.
Vlan Name	Name of the VLAN for which local switching is performed.
Mode	Value of the 802.1Q tag used for the VLAN.
ap numbers	The index numbers of the AP

See Also

- **set ap local-switching vlan-profile** on page 12-242
- **clear vlan-profile** on page 6-71
- **set vlan-profile** on page 6-75

Use Quality of Service (QoS) commands to configure packet prioritization in MSS. Packet prioritization ensures that MX switches and MPs give prefer

```
MX# clear qos
success: change accepted.
```

The following command resets the mapping used to classify packets with DSCP value 44:

```
MX# clear qos dscp-to-qos-map 44
success: change accepted.
```

clear qos-profile

Clears a QoS profile from the configuration.

Syntax **clear qos-profile** *profile-name*

Defaults None

Access Enabled

History Introduced in MSS Version 6.2.

Examples To clear a QoS profile with the profile name, best_voice, from the MSS configuration, use the following command:

```
MX# clear qos-profile best_voice
success: change accepted
```

set qos cos-to-dscp-map

Changes the value that MSS maps an internal QoS value when marking outbound packets.

Syntax **set qos cos-to-dscp-map** *level* **dscp** *dscp-value*

level	Internal CoS value. You can specify a number from 0 to 7.
dscp *dscp-value*	DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63.

Defaults The defaults are listed by the **show qos** command.

Access Enabled.

History Introduced in MSS Version 4.1.

Examples The following command maps internal CoS value 5 to DSCP value 50:

```
MX# set qos cos-to-dscp-map 5 dscp 50
warning: cos 5 is marked with dscp 50 which will be classified as cos 6
```

If the change results in a change to CoS, MSS displays a warning message indicating the change. In this example, packets receiving CoS 5 upon ingress are marked with a DSCP value equivalent to CoS 6 upon egress.

See Also

- **set qos dscp-to-cos-map** on page 7-86
- **show qos** on page 7-88

set qos dscp-to-cos-map

Changes the internal QoS value that MSS maps to a packet DSCP value when classifying inbound packets.

Syntax **set qos dscp-to-cos-map** *dscp-range* **cos** *level*

Defaults The defaults are listed by the **show qos** command.

Access Enabled.

History Introduced in MSS Version 4.1.

Examples The following command maps DSCP values 40-56 to internal CoS value 6:

```
MX# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be classified as cos 7
warning: cos 7 is marked with dscp 56 which will be classified as cos 6
```

As shown in this example, if the change results in a change to CoS, MSS displays a warning message indicating the change.

See Also

- **set qos cos-to-dscp-map** on page 7-86
- **show qos** on page 7-88

set qos-profile

Configures QoS parameters to apply to multiple clients.

Syntax **set qos-profile** *profile-name* **[[access-category [background | best effort | video | voice]|[cos** *static-cos-value***][max-bandwidth** *max-bw-kb***][use-client-dscp enable | disable]]**

Defaults None

Access Enabled

History Q3-awla(e)3.6ela(e)ry63.os 7

show qos

Displays the MX QoS settings.

Syntax **show qos** [**default**]

default Displays the default mappings.

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.1.

Examples The following command displays the default QoS settings:

```
MX# show qos default

Ingress QoS Classification Map (dscp-to-cos)

Ingress DSCP       CoS Level
================================================================================
       00-09       0    0    0    0    0      0    0    0    1    1
       10-19       1    1    1    1    1      1    2    2    2    2
       20-29       2    2    2    2    3      3    3    3    3    3
       30-39       3    3    4    4    4      4    4    4    4    4
       40-49       5    5    5    5    5      5    5    5    6    6
       50-59       6    6    6    6    6      6    7    7    7    7
       60-63       7    7    7    7


Egress QoS Marking Map (cos-to-dscp)

CoS Level              0      1      2      3      4      5      6      7
================================================================================
Egress DSCP            0      8     16     24     32     40     48     56
Egress ToS byte      0x00   0x20   0x40   0x60   0x80   0xA0   0xC0   0xE0
```

See Also **show qos dscp-table** on page 7-88

show qos dscp-table

Displays a table that maps Differentiated Services Code Point (DSCP) values to the equivalent combinations of IP precedence values and IP ToS values.

Syntax **show qos dscp-table**

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0 as the **show security acl dscp** command and renamed in MSS Version 4.1.

Examples The following command displays the table:

```
MX# show qos dscp-table

DSCP           TOS            precedence    tos
dec  hex       dec  hex
-----------------------------------------------
```

```
  0  0x00        0  0x00              0      0
  1  0x01        4  0x04              0      2
  2  0x02        8  0x08              0      4
...
 63  0x3f      252  0xfc              7     14
```

See Also **show qos** on page 7-88

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), aliases, and to ping a host or trace a route. This chapter presents IP services commands alphabetically. Use the following table to locate commands in this chapter based on their use.

	clear timezone on page 8-99
	clear summertime on page 8-98
NTP	**set ntp** on page 8-113
	set ntp server on page 8-114
	set ntp update-interval on page 8-114
	show ntp on page 8-139
	clear ntp server on page 8-95
	clear ntp update-interval on page 8-96
ARP	**set arp** on page 8-101
	set arp agingtime on page 8-101
	show arp on page 8-130
SNMP	**set snmp protocol** on page 8-123
	set snmp security on page 8-123
	set snmp community on page 8-115
	set snmp community group on page 8-116
	set snmp usm on page 8-125
	set snmp notify profile on page 8-116
	set snmp notify target on page 8-120
	set ip snmp server on page 8-110
	show snmp status on page 8-141
	show snmp community on page 8-140
	show snmp usm on page 8-142
	show snmp notify profile on page 8-141
	show snmp notify target on page 8-141
	show snmp counters on page 8-140
	show

clear interface

Removes an IP interface.

Syntax **clear interface** *vlan-id* **ip**

Defaults None.

Access En

History

See Also

- **clear ip dns server** on page 8-94
- **set ip dns** on page 8-106
- **set ip dns domain** on page 8-106
- **set ip dns server** on page 8-107
- **show ip dns** on page 8-135

clear ip dns server

Removes a DNS server from an MX configuration.

Syntax **clear ip dns server** *ip-addr*

Defaults None.

Access Enabled.

History Inl41.1265 l1s2 inpaMSS Veset iExamples

History

Version 1.0	Command introduced.
Version 1.1	❑ and / options added. These options are required in MSS version 1.1. ❑ option added, because MSS 1.1 supports multiple routes to the same destination. This option is required in MSS version 1.1.

Examples The following command removes the route to destination 10.10.10.68/24 through router 10.10.10.1:

```
MX# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

See Also

- **set ip route** on page 8-108
- **show ip route** on page 8-137

clear ip telnet

Resets the Telnet server TCP port number to the default value. An MX listens for Telnet management traffic on the Telnet server port.

Syntax **clear ip telnet**

Defaults The default Telnet port number is 23.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command resets the TCP port number for Telnet management traffic to its default:

```
MX# clear ip telnet
success: change accepted.
```

See Also

- **set ip https server** on page 8-108
- **set ip telnet** on page 8-112
- **set ip telnet server** on page 8-112
- **show ip https** on page 8-136
- **show ip telnet** on page 8-138

clear ntp server

Removes an NTP server from an MX configuration.

Syntax **clear ntp server** {*ip-addr* | **all**}

ip-addr	IP address of the server to remove, in dotted decimal notation.
all	Removes all NTP servers from the configuration.

Defaults None.

Access Enabled.

History Introduced in(3:MSS Ve9(rsi41 0.( )]TJ/TT4 1 Tf8.1356 0 0 9 89.669)7234 Tm-.0302 Tc-1034 TwExample

See Also

- **set snmp community** on page 8-115
- **show snmp community** on page 8-140

clear snmp notify profile

clear sn3eW 6y profile

Clears an SNMP notification profile.

Syntax **clear snmp notify profile** *profile-name*

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command clears notification profile :

```
MX# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```

See Also

- **set snmp 3 0 0 15.96 68.TD.0027 40.34 Tm.0016 Tc.0004n MSS96 9o /TT4 1 Tf.0g5e 8-115**

See Also

- **set snmp notify target** on page 8-120
- **show snmp notify target** on page 8-141

clear snmp trap receiver

This command is deprecated in MSS Version 4.0. To clear an SNMP notification target (also called), see **clear snmp notify target** on page 8-97.

clear snmp usm

Clears an SNMPv3 user.

Syntax **clear snmp usm** *usm-user-name*

- **show timedate** on page 8-142
- **show timezone** on page 8-143

clear system ip-address

Clears the system IP address.

Syntax **clear system ip-address**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Clearing the system IP address can interfere with system tasks using the system IP address, including the following:

- Mobility Domain operations
- Topology reporting for dual-homed MPs
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples To clear the system IP address, type the following command:

```
MX# clear system ip-address
success: change accepted.
```

See Also

- **set system ip-address** on page 8-128
- **show system** on page 4-40

clear timezone

Clears the time offset for the MX real-time clock from Coordinated Universal Time (UTC). UTC is also know as Greenwich Mean Time (GMT).

Syntax **clear timezone**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples To return the MX real-time clock to UTC, type the following command:

```
MX#
```

See Also

Syntax **clear summertime** on page 8-98

- **set summertime** on page 8-127
- **set timedate** on page 8-128
- **set timezone** on page 8-129
- **show summertime** on page 8-142
- **show timedate** on page 8-142
- **show timezone** on page 8-143

ping

Tests IP connectivity between an MX and another device. MSS sends an Internet Control Message Protocol (ICMP) echo packet to the specified device and listens for a reply packet.

Syntax **ping** *host* [**count** *num-packets*] [**dnf**] [**flood**] [**interval** *time*] [**size** *size*][**tos** *tos*] [**user count** *num-packets*] [**dnf**] [**flood**] [**interval** *time*] [**size** *size*][**tos** *tos*]]

host	IP address, MAC address, hostname, alias, or user to ping.
count *num-packets*	Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, MSS pings continuously until you interrupt the command.
dnf	Enables the Do Not Fragment bit in the ping packet to prevent fragmenting the packet.
flood	Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater. **Note:** Use the **flood** option sparingly. This option creates a lot of traffic and can affect other traffic on the network.
interval *time*	Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000.
size *size*	Packet size, in bytes. You can specify from 56 through 65,507. **Note:** Because the MX adds header information, the ICMP packet size is 8 bytes larger than the specified size.
tos *tos*	Set the tos byte in the IP header. You can specify an integer from 0 to 255.
user	Interpret 'host' argument as a user name.

Defaults

- **count**—5.
- **dnf**—Disabled.
- **interval**—100 (one tenth of a second)
- **size**—56.

Access Enabled.

History

Version 1.0	Command introduced.
Version 3.0	**user** option deprecated.
Version 7.0	**tos** and **user** options added.

Usage To stop a **ping** command in progress, press Ctrl+C.

An MX cannot ping its IP address. MSS does not support this.

Examples The following command pings a device that has IP address 10.1.1.1:

```
MX# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

See Also **traceroute** on page 8-144

set arp

Adds an ARP entry to the ARP table.

Syntax **set arp** {**permanent** | **static** | **dynamic**} *ip-addr mac-addr*

permanent	Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle.
dynamic	Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle.
ip-addr	IP address of the entry, in dotted decimal notation.
mac-addr	MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
MX# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

See Also

- **set arp agingtime** on page 8-101
- **show arp** on page 8-130

set arp agingtime

Changes the aging timeout for dynamic ARP entries.

Syntax **set arp agingtime** *seconds*

seconds	Number of seconds an entry can remain unused before MSS removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0.

Defaults The default aging timeout is 1200 seconds.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the **set arp agingtime 1200** command.

Examples The following command changes the ARP aging timeout to 1800 seconds:

```
MX# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
MX# set arp agingtime 0
success: set arp aging time to 0 seconds
```

See Also

- **set arp** on page 8-101
- **show arp** on page 8-130

set interface

Configures an IP interface on a VLAN.

Syntax **set interface** *vlan-id* **ip** {*ip-addr mask* | *ip-addr/mask-length*}

vlan-id	VLAN name or number.
ip-addr mask	IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
ip-addr/mask-length	IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You can assign one IP interface to each VLAN.

If an interface is already configured on the specified VLAN, this command replaces the interface. If you replace an interface in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations
- Topology reporting for dual-homed MPs
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples The following command configures IP interface 10.10.10.10/24 on VLAN :

```
MX# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN :

```
MX# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

See Also

- **clear interface** on page 8-92
- **set interface status** on page 8-105
- **show interface** on page 8-133

set interface dhcp-client

Configures the DHCP client on a VLAN and allows the VLAN to obtain an IP interface from a DHCP server.

Syntax **set interface** *vlan-id* **ip dhcp-client** {**enable** | **disable**}

vlan-id	VLAN name or number.
enable	Enables the DHCP client on the VLAN.
disable	Disables the DHCP client on the VLAN.

Defaults The DHCP client is enabled by default on an unconfigured MXR-2 when the factory reset switch is pressed and held during power on.

The DHCP client is disabled by default on all other MX models, and is disabled on an MXR-2 if it is already configured, or the factory reset switch is not pressed and held during power on.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. (See **set interface dhcp-server** on page 8-103.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

Examples The following command enables the DHCP client on VLAN :

```
MX# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

See Also

- **clear interface** on page 8-92
- **show dhcp-client** on page 8-130
- **show interface** on page 8-133

set interface dhcp-server

Configures the MSS DHCP server.

Table 0-1.

Syntax **set interface** *vlan-id* **ip dhcp-server** [**enable** | **disable**] [**start** *ip-addr1* **stop** *ip-addr2*] [**dns-domain** *domain-name*] [**primary-dns** *ip-addr* [**secondary-dns** *ip-addr*]] [**default-router** *ip-addr*]

Defaults The DHCP server is enabled by default on a new (unconfigured) MXR-2, MX-8, MX-200, or MX-216, in order to provide an IP address to the host connected to the MX for access to the Web Quick Start. On all MX models, the DHCP server is enabled and cannot be disabled for directly connected MPs.

The DHCP server is disabled by default for any other use.

Access Enabled.

History

Usage By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Specification of the DNS domain name, DNS servers, and default router are optional. If you omit one or more of these options, the MSS DHCP server uses oath values configured elsewhere on the

- **set ip dns domain** on page 8-106
- **set ip dns server** on page 8-107
- **show dhcp-server** on page 8-131

set interface status

Administratively disables or reenables an IP interface.

Syntax **set interface** *vlan-id* **status** {**up** | **down**}

Defaults IP interfaces are enabled by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command disables

set ip dns

Enables or disables DNS on an MX.

Syntax **set ip dns** {**enable** | **disable**}

Defaults DNS is disabled by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command enables DNS on an MX:

```
MX# set ip dns enable
Start DNS Client
```

See Also

- **clear ip dns domain** on page 8-93
- **clear ip dns server** on page 8-94

m6654 Tw[4(t i( )-p d(s dom)-4.(pa.9(in)]TJ/TT6 1 T129.6712 0 TD.0006 Tc.0718 Tw[on)6(pa)5.4(ge)-275.2(8)-5.106(4)]TJ/F1 1 Tf6.96 0 0 6.96 89.64447

See Also

- **set ip dns server** on page 8-107
- **show ip dns** on page 8-135

set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

Syntax **set ip dns server** *ip-addr* {**primary** | **secondary**}

ip-addr	IP address of a DNS server, in dotted decimal or CIDR notation.
primary	Defines the server as the primary server that MSS always consults first for resolving DNS queries.
secondary	Defines the server as a secondary server. MSS consults a secondary server only if the primary server does not reply.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You can configure an MX to use one primary DNS server and up to five secondary DNS servers.

Examples The following commands configure an MX to use a primary DNS server and two secondary DNS servers:

```
MX# set ip dns server 10.10.10.50/24 primary
success: change accepted.

MX# set ip dns server 10.10.20.69/24 secondary
success: change accepted.

MX# set ip dns server 10.10.30.69/24 secondary
success: change accepted.
```

See Also

- **clear ip dns domain** on page 8-93
- **clear ip dns server** on page 8-94
- **set ip dns** on page 8-106
- **set ip dns domain** on page 8-106
- **show ip dns** on page 8-135

Defaults None.

Access Enabled.

History

Usage MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is available. If one of the added routes can resolve the static route, MSS can use the static route.

- **show ip route** on page 8-137

set ip snmp server

Enables or disables the SNMP service on the MX.

Syntax **set ip snmp server** {**enable** | **disable**}

enable Enables the SNMP service.

disable Disables the SNMP service.

Defaults The SNMP service is disabled by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command enables the SNMP server on an MX:

```
MX# set ip snmp server enable
success: change accepted.
```

See Also

- **clear snmp trap receiver** on page 8-98
- **set port trap** on page 5-58
- **set snmp community** on page 8-115
- **set snmp trap** on page 8-124
- **set snmp trap receiver** on page 8-124
- **show snmp configuration** on page 8-140

set ip ssh

Changes the TCP port number on which an MX listens for Secure Shell (SSH) management traffic.

Table 0-3.

If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.

Syntax **set ip ssh port** *port-num*

port-num TCP port number.

Defaults The default SSH port number is 22.

Access Enabled.

History Introduced in MSS Version 2.0.

Examples The following command changes the SSH port number on an MX to 6000:

```
MX# set ip ssh port 6000
success: change accepted.
```

set ip telnet

Changes the TCP port number that an MX listens for Telnet management traffic.

Table 0-5.

Syntax **set ip telnet** *port-num*

Defaults The default Telnet port number is 23.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command changes the Telnet port number on an MX to 5000:

```
MX# set ip telnet 5000
success: change accepted.
```

See Also

- **clear ip telnet** on page 8-95
- **set ip https server** on page 8-108
- **set ip telnet server** on page 8-112
- **show ip https** on page 8-136
- **show ip telnet** on page 8-138

set ip telnet server

Enables the Telnet server on an MX.

Syntax **set ip telnet server** {**enable** | **disable**}

Defaults The Telnet server is disabled by default.

Access Enabled.

set ntp server

Configures an MX to use an NTP server.

Syntax **set ntp server** *ip-addr*

ip-addr IP address of the NTP server, in dotted decimal notation.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305,

.

To use NTP, you also must enable the NTP client with the **set ntp** command.

Examples The following command configures an MX to use NTP server 192.168.1.5:

```
MX# set ntp server 192.168.1.5
```

See Also

- **clear ntp server** on page 8-95
- **clear ntp update-interval** on page 8-96
- **set ntp** on page 8-113
- **set ntp update-interval** on page 8-114
- **show ntp** on page 8-139

set ntp update-interval

Changes how often an MX sends quer.1ies to the NTP servers for updates.

Syntax **set ntp update-interval** *seconds*

seconds

Defaults The default NTP update interval is 64 seconds.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command changes the NTP update interval to 128 seconds:

```
MX# set ntp update-interval 128
success: change accepted.
```

See Also

- **clear ntp server** on page 8-95
- **clear ntp update-interval** on page 8-96
- **set ntp** on page 8-113
- **set ntp server** on page 8-114
- **show ntp** on page 8-139

set snmp community

Configures a community string for SNMPv1 or SNMPv2c.

Syntax **set snmp community name** *comm-string*
access {**read-only** | **read-notify** | **notify-only** | **read-write** | **notify-read-write**}

Defaults None.

Access Enabled.

History

Usage SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. Trapeze Networks recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings and .

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt

notification-type Name of the notification type:

- **ApNonOperStatusTraps**—Generated to indicate an MP radio is nonoperational.
- **ApOperRadioStatusTraps**—Generated when the status of an MP radio changes.
- ApRejectLicenseExceededTraps–Generated when the number of MPs exceeds the licenses.
- **AuthenTraps—**Generated when the MX switch's SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps—**Generated when the RF Auto-Tuning feature changes the channel on a radio.
- **AutoTuneRadioPowerChangeTraps—**Generated when the RF Auto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps—**Generated when a client's attempt to associate with a radio fails.
- ClientAssociationSuccessTraps—Generated when a client associates successfully.
- **ClientAuthenticationSuccessTraps—**Generated when a client successfully authenticates on the network.
- **ClientAuthenticationFailureTraps—**Generated when authentication fails for a client.
- **ClientAuthorizationSuccessTraps—**Generated when a client is successfully authorized.
-
- **ClientAuthorizationFailureTraps—**Generated when authorization fails for a client.
- **ClientClearedTraps—**Generated when a client's session is cleared.
- **ClientDeAssociationTraps—**Generated when a client is dissociated from a radio.
- **ClientDeAuthenticationTraps—Generated when a client deauthenticates from a radio.**
- **ClientDisconnectTraps—Generated when a client disconnects from the radio.**
- **ClientDot1xFailureTraps—**Generated when a client experiences an 802.1X failure.
- ClientDynAuthorChangeFailureTraps—
- ClientDynAuthorChangeSuccessTraps—
- ClientIPAddrChangeTraps—Generated when the IP address for a client changes.
- **ClientRoamingTraps—**Generated when a client roams.
- ConfigurationsSavedTraps—Generated when a configuration is saved on an MX.
- **CounterMeasureStartTraps—**Generated when MSS begins countermeasures against a rogue access point.

notification-type (cont.)

- **CounterMeasureStopTraps—**Generated when MSS stops countermeasures against a rogue access point.
- **DeviceFailTraps—**Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps—**Generated when a device returns to its normal state.
- **LinkDownTraps—**Generated when the link is lost on a port.
- **LinkUpTraps—**Generated when the link is detected on a port.
- **MichaelMICFailureTraps—**Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
- **MobilityDomainFailBackTraps—Generated when a primary seed returns to primary status after a failover to a secondary seed.**
- **MobilityDomainFailOverTraps—Generated when a secondary mobility domain seed becomes the primary seed when a failover occurs on the network.**
- **MobilityDomainJoinTraps—**Generated when the MX switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.
- **MobilityDomainTimeoutTraps—**Generated when a timeout occurs after an MX switch has unsuccessfully tried to communicate with a seed member.
- **PoEFailTraps—**Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when MSS detects an ad-hoc user.
- RFDetectAdhocUserDisappearTraps—Generated when an ad hoc user is no longer detected on the network.
- RFDetectBlacklistedTraps—Generated when blacklisted APs are detected on the network.
- RFDetectClassificationChangeTraps—Generated when the classification of a device changes.
- **RFDetectRogueDeviceTraps**—Generated when MSS detects a rogue device .
- **RFDetectRogueDeviceDisappearTraps**—Generated when a rogue device is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.

)

- **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueDeviceTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDeviceDisappearTraps**—Generated when an interfering device is no longer detected.
- **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of a Trapeze MP, but without the spoofed MP's signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
- RFDetectSuspectDeviceDisappearTraps—Generated when a suspect device disappears from the network.
- RFDetectSuspectDeviceTraps—Generated when a wireless device not on the list of permitted vendors is detected.
-

all Sends or drops all notifications.

Defaults A default notification profile (named) is already configured on the MX. All notifications in the default profile are dropped by default.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command changes the action in the default notification profile from **drop** to **send** for all notification types:

```
MX# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile , and change the action to **send** for all RF detection notification types:

```
MX# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.

MX# set snmp notify profile snmp_rfdetect send RFDetectAdhocUserDisappearTraps

success: change accepted

MX# set snmp notify profile snmp_rfdetect send RFDetectBlacklistedTraps
success: change accepted

MX# set snmp notify profile snmpprof_rfdetect send RFDetectClientViaRogueWiredAPTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectInterferingRogueAPTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectInterferingRogueDisappearTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectRogueDisappearTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedMacAPTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedSsidAPTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedAPTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedOuiTraps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedSsidTraps
success: change accepted.
```

See Also

- **clear snmp notify profile** on page 8-97
- **set ip snmp server** on page 8-110
- **set snmp community** on page 8-115
- **set snmp notify target** on page 8-120
- **set snmp protocol** on page 8-123
- **set snmp security** on page 8-123
- **set snmp usm** on page 8-125
- **show snmp notify profile** on page 8-141

set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device that the MX sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

SNMPv3 with Informs

To configure a notification target for informs from SNMPv3, use the following command:

Syntax **set snmp notify target** *target-num ip-addr*[:*udp-port-number*]
usm inform user *username*
snmp-engine-id {**ip** | **hex** *hex-string*}
[**profile** *profile-name*]
[**security** {**unsecured** | **authenticated** | **encrypted**}]
[**retries** *num*]
[**timeout** *num*]

target-num	ID for the target. This ID is local to the MX and does not need to correspond to a value on the target. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
username	USM username. This option is applicable only when the SNMP version is **usm**. If the user sends informs rather than traps, you also must specify the **snmp-engine-id** of the target.
snmp-engine-id {**ip** | **hex** *hex-string*}	SNMP engine ID of the target. Specify **ip** if the target SNMP engine ID is based on the IP address. If the target SNMP engine ID is a hexadecimal value, use **hex** to specify the value.
profile *profile-name*	Notification profile that the SNMP user use to specify the notification types to send or drop.
security {**unsecured** | **authenticated** | **encrypted**}	Specifies the security level, and is applicable only when the SNMP version is **usm**: ❑ **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default. ❑ **authenticated**—Message exchanges are authenticated, but are not encrypted. ❑ **encrypted**—Message exchanges are authenticated and encrypted.
retries *num*	Specifies the number of times the MSS SNMP engine resends a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
timeout *num*	Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv3 with Traps

To configure a notification target for traps from SNMPv3, use the following command:

Syntax **set snmp notify target** *target-num ip-addr*[:*udp-port-number*]
usm trap user *username*
[**profile** *profile-name*]
[**security** {**unsecured** | **authenticated** | **encrypted**}]

target-num	ID for the target. This ID is local to the MX and does not need to correspond to a value on the target. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
username	USM username. This option is applicable only when the SNMP version is **usm**.
profile *profile-name*	Notification profile this SNMP user uses to specify the notification types to send or drop.
security {**unsecured** | **authenticated** | **encrypted**}	Specifies the security level, and is applicable only when the SNMP version is **usm**: ❑ **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default. ❑ **authenticated**—Message exchanges are authenticated, but are not encrypted. ❑ **encrypted**—Message exchanges are authenticated and encrypted.

SNMPv2c with Informs

To configure a notification target for informs from SNMPv2c, use the following command:

Syntax **set snmp notify target** *target-num ip-addr*[:*udp-port-number*]
v2c *community-string* **inform**
[**profile** *profile-name*]
[**retries** *num*]
[**timeout** *num*]

target-num	ID for the target. This ID is local to the MX and does not need to correspond to a value on the target. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
community-string	Community string.
profile *profile-name*	Notification profile this SNMP user will use to specify the notification types to send or drop.
retries *num*	Specifies the number of times the MSS SNMP engine resends a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
timeout *num*	Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv2c with Traps

To configure a notification target for traps from SNMPv2c, use the following command:

Syntax **set snmp notify target** *target-num ip-addr*[:*udp-port-number*]
v2c *community-string* **trap**
[**profile** *profile-name*]

SNMPv1 with Traps

To configure a notification target for traps from SNMPv1, use the following command:

Syntax **set snmp notify target** *target-num ip-addr*[:*udp-port-number*]
v1 *community-string*
[**profile** *profile-name*]

Defaults The default UDP port number on the target is 162. The default minimum required security level is **unsecured**. The default number of retries is 0 and the default timeout is 2 seconds.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage The **inform** or **trap** option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the MX ~~switch~~. Use **inform** if you want acknowledgements. Use **trap** if you do not want acknowledgements. The **inform** option is applicable to SNMP version **v2c** or **usm** only.

Examples The following command configures a notification target for acknowledged notifications:

```
MX#
```

Syntax **set snmp security**
{**unsecured** | **authenticated** | **encrypted** | **auth-req-unsec-notify**}

unsecured	SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c.
authenticated	SNMP message exchanges are authenticated but are not encrypted.
encrypted	SNMP message exchanges are authenticated and encrypted.
auth-req-unsec-notify	SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

Defaults By default, MSS allows nonsecure (**unsecured**) SNMP message exchanges.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

Examples The following command sets the minimum level of SNMP security allowed to authentication encryption:

```
MX# set snmp security encrypted
success: change accepted.
```

See Also

- **set ip snmp server** on page 8-110
- **set snmp community** on page 8-115
- **set snmp notify target** on page 8-120
- **set snmp notify profile** on page 8-116
- **set snmp protocol** on page 8-123
- **set snmp usm** on page 8-125
- **show snmp status** on page 8-141

set snmp trap

This command is deprecated in MSS Version 4.0. To enable or disable SNMP notifications, configure a notification profile. See **set snmp notify profile** on page 8-116.

set snmp trap receiver

This command is deprecated in MSS Version 4.0. To configure an SNMP notification target (also called), see **set snmp notify target** on page 8-120.

set snmp usm

Creates a USM user for SNMPv3.

Table 0-3.

This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the **set snmp community** command to configure community strings.

Syntax **set snmp usm** *usm-user-name* **snmp-engine-id** {**ip** *ip-addr* | **local** | **hex** *hex-string*} **access** {**read-only** | **read-notify** | **notify-only** | **read-write** | **notify-read-write**} **auth-type** {**none** | **md5** | **sha**} {**auth-pass-phrase** *string* | **auth-key** *hex-string*} **encrypt-type** {**none** | **des** | **3des** | **aes**} {**encrypt-pass-phrase** *string* | **encrypt-key** *hex-string*}

usm-user-name	Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces.
snmp-engine-id {**ip** *ip-addr* | **local** | **hex** *hex-string*}	Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify **local** as the engine ID. ❑ **hex** —ID is a hexadecimal string. ❑ **ip** —ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address. ❑ **local**—Uses the value computed from the switch's system IP address.
access {**read-only** | **read-notify** | **notify-only** | **read-write** | **notify-read-write**}	Specifies the access level of the user: ❑ **read-only**—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them. ❑

auth-type {**none** | **md5** | **sha**} {**auth-pass-phrase** *string* | **auth-key** *hex-string*}	Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following: ❑ **none**—No authentication is used. ❑ **md5**—Message-digest algorithm 5 is used. ❑ **sha**—Secure Hashing Algorithm (SHA) is used. If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key. ❑ To specify a passphrase, use the **auth-pass-phrase** option. The string can be from 8 to 32 alphanumeric characters long, with no spaces. ❑ To specify a key, use the **auth-key** option.
encrypt-type {**none** | **des** | **3des** | **aes**} {**encrypt-pass-phrase** *string* | **encrypt-key** *hex-string*}	Specifies the encryption type used for SNMP traffic. You can specify one of the following: ❑ **none**—No encryption is used. This is the default. ❑ **des**—Data Encryption Standard (DES) encryption is used. ❑ **3des**—Triple DES encryption is used. ❑ **aes**—Advanced Encryption Standard (AES) encryption is used. If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key. ❑ To specify a passphrase, use the **encrypt-pass-phrase** option. The string can be from 8 to 32 alphanumeric characters long, with no spaces. ❑ To specify a key, use the **encrypt-key** option.

Defaults No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is **read-only**, and the default authentication and encryption types are both **none**.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command creates USM user , associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
MX# set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user , which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
MX# set snmp usm securesnmpmgr1 snmp-engine-id ip 192.168.40.2 auth-type sha auth-pass-phrase
    myauthpword encrypt-type 3des encrypt-pass-phrase mycryptpword
success: change accepted.
```

See Also

- **clear snmp usm** on page 8-98
- **set ip snmp server** on page 8-110
- **set snmp community** on page 8-115
- **set snmp notify target** on page 8-120
- **set snmp notify profile** on page 8-116
- **set snmp protocol** on page 8-123
- **set snmp security** on page 8-123
- **show snmp usm** on page 8-142

set summertime

Offsets the real-time clock of an MX by +1 hour and returns it to standard time for daylight savings time or a similar summertime period.

Syntax **set summertime** *summer–name* [**start** *week weekday month hour min* **end** *week weekday month hour min*]

summer–name	Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like.
start	

Defaults If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You must first set the time zone with the **set timezone** command for the offset to work properly without the start and end values.

Configure summertime you set the time and date. Otherwise, the summertime adjustment of the time makes the time incorrect, if the date is within the summertime period.

Examples To enable summertime and set the summertime time zone to (Pacific Daylight Time), type the following command:

```
MX-20# set summertime PDT
success: change accepted
```

See Also

- **clear summertime** on page 8-98
- **clear timezone** on page 8-99
- **set timedate** on page 8-128
- **set timezone** on page 8-129
- **show summertime** on page 8-142
- **show timedate** on page 8-142
- **show timezone** on page 8-143

Configure summertime

Syntax **show dhcp-client**

Defaults None.

Access All.

History Introduced in MSS Version 4.0.

Examples The following command displays DHCP client information:

```
MX# show dhcp-client
 Interface:            corpvlan(4)
 Configuration Status: Enabled
 DHCP State:           IF_UP
 Lease Allocation:     65535 seconds
 Lease Remaining:      65532 seconds
 IP Address:           10.3.1.110
 Subnet Mask:          255.255.255.0
 Default Gateway:      10.3.1.1
 DHCP Server:          10.3.1.4
```

Syntax **show dhcp-server** [**interface** *vlan-id*] [**verbose**]

Defaults None.

Access All.

History Introduced in MSS Version 4.0.

Examples The following command displays the addresses leased by the MSS DHCP server:

```
MX# show dhcp-server
VLAN Name           Address         MAC               Lease Remaining (sec)
---- -------------- --------------- ----------------- --------------------
   1 default        10.10.20.2      00:01:02:03:04:05                 12345
   1 default        10.10.20.3      00:01:03:04:06:07                  2103
   2 red-vlan       192.168.1.5     00:01:03:04:06:08                   102
   2 red-vlan       192.168.1.7     00:01:03:04:06:09                 16789
```

The following command displays configuration and status information for each VLAN that the DHCP server is configured:

```
MX# show dhcp-server verbose
Interface:        0 (Direct AP)
 Status:           UP
 Address Range:    10.0.0.1-10.0.0.253

 Interface:            default(1)
 Status:               UP
 Address Range:        10.10.20.2-10.10.20.254
Hardware Address:     00:01:02:03:04:05
   State:                BOUND
   Lease Allocation:     43200 seconds
   Lease Remaining:      12345 seconds
   IP Address:           10.10.20.2
   Subnet Mask:          255.255.255.0
```

Interface	VLAN name and number.
Status	Status of the interface: ❑ UP ❑ DOWN
Address Range	Range from which the server can lease addresses.
Hardware Address	MAC address of the DHCP client.
State	State of the address lease: ❑ SUSPEND—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected. ❑ CHECKING—MSS is using ARP to verify whether the address is available. ❑ OFFERING—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address. ❑ BOUND—The client accepted the address. ❑ HOLDING—The address is already in use and is therefore unavailable.
Lease Allocation	Duration of the address lease, in seconds.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address leased to the client.
Subnet Mask	Network mask of the IP address leased to the client.
Default Router	Default router IP address in

See Also **set interface dhcp-server** on page 8-103

show interface

Displays the IP interfaces configured on the MX.

Syntax **show interface** [*vlan-id*]

Defaults If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

Access All.

History

Usage The IP interface table flags an address assigned by a DHCP server with an asterisk (*).

Examples The following command displays all the IP interfaces configured on an MX:

Name	Alias string.
IP Address	IP address associated with the alias.

See Also

- **clear ip alias** on page 8-93
- **set ip alias** on page 8-105

show ip dns

Displays the DNS servers used by the MX.

Syntax **show ip dns**

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command displays the DNS information:

```
MX# show ip dns
Domain Name: example.com
DNS Status: enabled
IP Address                Type
----------------------------------
10.1.1.1                  PRIMARY
10.1.1.2                  SECONDARY
10.1.2.1                  SECONDARY
```

Table 8– 3 describes the fields in this display.

Domain Name	Default domain name configured on the MX
DNS Status	Status of the MX DNS client: ❑ Enabled ❑ Disabled
IP Address	IP address of the DNS server
Type	Server type: ❑ PRIMARY ❑ SECONDARY

See Also

- **clear ip dns domain** on page 8-93
- **clear ip dns server** on page 8-94
- **set ip dns** on page 8-106
- **set ip dns domain** on page 8-106
- **set ip dns server** on page 8-107

show ip https

Displays information about the HTTPS management port.

Syntax **show ip https**

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command shows the status and port number for the HTTPS management interface to the MX switch:

```
MX> show ip https
HTTPS is enabled
HTTPS is set to use port 443

Last 10 Connections:
 IP Address     Last Connected          Time Ago (s)
------------    ----------------------  ------------
10.10.10.56     2003/05/09 15:51:26 pst          349
```

Table 8– 4 describes the fields in this display.

See Also

- **clear ip telnet** on page 8-95
-

show ip route

Displays the IP route table on the MX.

Syntax **show ip route** [*destination*]

destination Route destination IP address, in dotted decimal notation.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Usage When you add an IP interface to an available VLAN, MSS adds direct and local routes for the interface to the route table. If the VLAN is down, MSS does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the **show vlan config** command to check the VLAN state.

If you add a static route and the route state is shown as Down, use the **show interface** command to verify that the MX has an IP interface in the default router subnet. MSS cannot resolve a static route unless one of the MX VLANs has an interface in the default router subnet. If the MX has such an interface but the static route is still down, use the **show vlan config** command to check the state of the VLAN ports.

Examples The following command shows all routes in an MX IP route table:

```
MX# show ip route
Router table for IPv4
Destination/Mask   Proto   Metric NH-Type Gateway         VLAN:Interface
_________________ _______ ______ _______ _______________ _______________

        0.0.0.0/ 0 Static       1 Router  10.0.1.17       Down
        0.0.0.0/ 0 Static       2 Router  10.0.2.17       vlan:2:ip
       10.0.2.1/24 IP           0 Direct                  vlan:2:ip
       10.0.2.1/32 IP           0 Direct                  vlan:2:ip:10.0.1.1/24
     10.0.2.255/32 IP           0 Direct                  vlan:2:ip:10.0.1.1/24
      224.0.0.0/ 4 IP           0 Local                   MULTICAST
```

Table 8– 5 describes the fields in this display.

- **set ip telnet server** on page 8-112
- **show ip https** on page 8-136

show ntp

Displays NTP client information.

Syntax **show ntp**

Defaults None.

Access All.

History

Examples To display NTP information for an MX, type the following command:

```
MX> show ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Fri Feb 06 2004, 12:02:57
```

Peer state	State of the NTP session from the point of view of the NTP server:	v.23(YT

See Also

- **clear ntp server** on page 8-95
- **clear summertime** on page 8-98
- **clear timezone** on page 8-99
- **set ntp** on page 8-113
- **set ntp server** on page 8-114
- **set summertime** on page 8-127
- **set timezone** on page 8-129
- **show timezone** on page 8-143

show snmp configuration

This command is deprecated in MSS Version 4.0. Use the **show snmp status** command instead.

show snmp community

Displays the configured SNMP community strings.

Syntax `show snmp community`

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

See Also

- **clear snmp community** on page 8-96
- **set snmp community** on page 8-115

show snmp counters

Displays SNMP statistics counters.

Syntax `show snmp counters`

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

show snmp notify profile

Displays SNMP notification profiles.

Syntax `show snmp notify profile`

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

- **clear snmp notify profile** on page 8-97
- **set snmp notify profile** on page 8-116

show snmp notify target

Displays SNMP notification targets.

Syntax `show snmp notify target`

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

See Also

- **clear snmp notify target** on page 8-97
- **set snmp notify target** on page 8-120

show snmp status

Displays SNMP version and status information.

Syntax `show snmp status`

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

See Also

- **set snmp community** on page 8-115
- **set snmp notify target** on page 8-120
- **set snmp notify profile** on page 8-116
- **set snmp protocol** on page 8-123
- **set snmp security** on page 8-123
- **set snmp usm** on page 8-125
- **show snmp community** on page 8-140
- **show snmp counters** on page 8-140
- **show snmp notify profile** on page 8-141
- **show snmp notify target** on page 8-141

Examples To display the time and date set on an MX real-time clock, type the following command:

```
MX-20#  show timedate
Sun Feb 29 2004, 23:59:02 PST
```

See Also

- **clear summertime** on page 8-98
- **clear timezone** on page 8-99
- **set summertime** on page 8-127
- **set timedate** on page 8-128
- **set timezone** on page 8-129
- **show summertime** on page 8-142
- **show timezone** on page 8-143

show timezone

Shows the time offset for the real-time clock from UTC on an MX.

Syntax **show timezone**

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples To display the offset from UTC, type the following command:

```
MX# show timezone
Timezone set to 'pst', offset from UTC is -8 hours
```

See Also

- **clear summertime** on page 8-98
- **clear timezone** on page 8-99
- **set summertime** on page 8-127
- **set timedate** on page 8-128
- **set timezone** on page 8-129
- **show summertime** on page 8-142
- **show timedate** on page 8-142

telnet

Opens a Telnet client session with a remote device.

Syntax **telnet** {*ip-addr* | *hostname*} [**port** *port-num*]

ip-addr	IP address of the remote device.
hostname	Hostname of the remote device.
port *port-num*	TCP port number that the TCP server on the remote device listens for Telnet connections.

Defaults MSS attempts to establish Telnet connections with TCP port 23 by default.

Access Enabled.

History Introduced in MSS Version 1.1.

Usage To end a Telnet session from the remote device, press Ctrl+t or type **exit** in the management session on the remote device. To end a client session from the local device, use the **clear sessions telnet client** command.

If the configuration of the MX on which you enter the **telnet** command has an ACL that denies Telnet client traffic, the ACL also denies access by the **telnet** command.

Examples In the following example, an administrator establishes a Telnet session with another MX and enters a command on the remote MX:

```
MX# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'

Copyright (c) 2002, 2003
        Trapeze Networks, Inc.

Username: username
Password: password

MX-remote> show vlan
                     Admin  VLAN  Tunl                          Port
VLAN Name            Status State Affin Port             Tag   State
---- --------------- ------ ----- ----- --------------- ----- -----
   1 default          Up     Up        5
                                         1                none Up
   3 red              Up     Up        5
  10 backbone         Up     Up        5
                                         21               none Up
                                         22               none Up
```

When the administrator presses Ctrl

Defaults

- **dnf**—Disabled
- **no-dns**—Disabled
- **port**—33434
- **queries**—3
- **size**—38
- **ttl**—30
- **wait**—5000

Access All.

History Introduced in MSS Version 1.0.

Usage To stop a **traceroute** command that is in progress, press Ctrl+C.

Examples The following example traces the route to host :

```
MX# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
```

!A	Communication administratively prohibited.
?	Unknown error occurred.

See Also **ping** on page 8-100

Use authentication, authorization, and accounting (AAA) commands to provide a secure network

system	Disables sending of Accounting-On and Accounting-Off messages to a RADIUS server, if previously enabled. When this command is entered, an Accounting-Off message is generated and sent to the server or server group specified with the **set accounting system** command.
user-glob	Single user or set of users with administrative access or network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.)

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 5.0	**system** option added
Version 7.0	**mac** and **web** options added

Examples The following command removes accounting services for authorized network user Nin:

```
MX# clear accounting dot1x Nin
success: change accepted.
```

See Also

- **set accounting {admin | console}** on page 9-160
- **set accounting system** on page 9-162
- **show accounting statistics** on page 9-198

clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web View.

Syntax **clear authentication admin** *user-glob*

user-glob	A single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.)

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Examples The following command clears authentication for administrator Jose:

```
MX# clear authentication admin Jose
success: change accepted.
```

See Also

- **clear authentication console** on page 9-150
- **clear authentication dot1x** on page 9-150
- **clear location policy** on page 9-153
- **clear authentication web** on page 9-152
- **set authentication admin** on page 9-163
- **show aaa** on page 9-189

clear authentication console

Removes an authentication rule for administrative access through the Console.

Syntax **clear authentication console** *user-glob*

user-glob	A single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.)

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Examples The following command clears authentication for administrator Regina:

```
MX# clear authentication console Regina
success: change accepted.
```

See Also

- **clear authentication admin** on page 9-149
- **clear authentication dot1x** on page 9-150
- **clear authentication mac** on page 9-151
- **clear authentication web** on page 9-152
- **set authentication console** on page 9-165
- **show aaa** on page 9-189

clear authentication dot1x

Removes an 802.1X authentication rule.

Syntax **clear authentication dot1x** {**ssid** *ssid-name* | **wired**} *user-glob*

ssid *ssid-name*	SSID name to which this authentication rule applies.
wired	Clears a rule used for access over an MX wired-authentication port.
user-glob	User-glob associated with the rule you are removing.

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 3.0	**ssid** and **wired** options added

Examples The following command removes 802.1X authentication for network users with usernames ending in who try to access SSID :

```
MX# clear authentication dot1x ssid finance *@thiscorp.com
```

See Also

- **clear authentication admin** on page 9-149
- **clear authentication console** on page 9-150
- **clear authentication mac** on page 9-151
- **clear authentication web** on page 9-152
- **set authentication dot1x** on page 9-166
- **show aaa** on page 9-189

clear authentication last-resort

Deprecated in MSS Version 5.0. The user is not required or supported in MSS Version 5.0. Instead, a user who accesses the network on an SSID by using the fallthru access type **last-resort** is automatically a user. The authorization attributes assigned to the user come from the default authorization attributes set on the SSID.

clear authentication mac

Removes a MAC authentication rule.

Syntax **clear authentication mac** {**ssid** *ssid-name* | **wired**} *mac-addr-glob*

ssid *ssid-name*	SSID name to apply the authentication.
wired	Clears a rule used for access over an MX wired-authentication port.
mac-addr-glob	MAC address glob associated with the rule you are removing.

Defaults None.

Access Enabled.

History

Examples The following command removes a MAC authentication rule for access to SSID by MAC addresses beginning with

```
MX# clear authentication mac ssid thatcorp aa:bb:cc:*
```

See Also

- **clear authentication admin** on page 9-149
- **clear authentication console** on page 9-150
- **clear authentication dot1x** on page 9-150
- **clear authentication web** on page 9-152
- **set authentication mac** on page 9-169
- **show aaa** on page 9-189

clear authentication proxy

Removes a proxy rule for third-party AP users.

Syntax

Defaults None.

Access Enabled.

History Introduced in MSS 3.0.

Examples The following command removes WebAAA for SSID and userglob :

```
MX# clear authentication web ssid research temp*@thiscorp.com
```

See Also

- **clear authentication admin** on page 9-149
- **clear authentication console** on page 9-150
- **clear authentication dot1x** on page 9-150
- **clear authentication mac** on page 9-151
- **set authentication web** on page 9-173
- **show aaa** on page 9-189

clear location policy

Removes a rule from the location policy on an MX switch.

Syntax **clear location policy** [*index* | **all**]

index	Index of MACE to clear (1...)
all	Clears all policies

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.1.

Version 1.1	Command introduced.
Version 7.0	replaced by the options and **all**.

Usage To determine the index numbers of location policy rules, use the **show location policy** command. Removing all the ACEs from the location policy disables this function on the MX.

Examples The following command removes location policy rule 4 from an MX location policy:

```
MX# clear location policy 4
success: clause 4 is removed.
```

See Also

- **set location policy** on page 9-174
- **show location policy** on page 9-200

clear mac-user

Removes a user profile from the local database on the MX for a user authenticated by a MAC address.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax `clear mac-user`

Examples The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

Access Enabled.

History Introduced in MSS 1.0.

Usage To remove a user from a MAC user group, use the **clear mac-user group** command.

Examples The following command deletes the MAC user group from the local database:

```
MX# clear mac-usergroup eastcoasters
success: change accepted.
```

See Also

- **clear mac-usergroup attr** on page 9-156
- **set mac-usergroup attr** on page 9-182
- **show aaa** on page 9-189

clear mac-usergroup attr

Removes an authorization attribute from a MAC user group in the local database on the MX, for a group of users who are authenticated by a MAC address.

(To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear mac-usergroup**

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Examples The following command removes the Mobility Profile for user Nin:

```
MX# clear mobility-profile Nin
success: change accepted.
```

See Also

- **set mobility-profile** on page 9-182
- **set mobility-profile mode** on page 9-184
- **show mobility-profile** on page 9-200

clear user

Removes a user profile from the local database on the MX.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear user** *username*

username	Username

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Usage Deleting the user profile from the database deletes the assignment of any profile attributes to the user.

Examples The following command deletes the user profile for user Nin:

```
MX# clear user Nin
success: change accepted.
```

See Also

- **set user** on page 9-184
- **show aaa** on page 9-189

clear user attr

Removes an authorization attribute from the user profile in the local database on the MX for a user with a password.

(To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

Syntax **clear user** *username* **attr** *attribute-name*

username	Username of a user with a password.
attribute-name	Name of an attribute used to authorize the user for a particular service or session characteristic. (For a list of authorization attributes, see Table 9– 9 on page 178.)

Defaults None.

Access Enabled.

FMXory

ine:

user 5 nusmX#m

Usage If a user's password has expired, or the user is unable to log in within the configured limit for login attempts, then the user is locked out of the system, and cannot gain access without the intervention of an adminstrator. Use this command to restore access to the user.

Examples The following command restores access to user Nin, who was previously locked out of the system:

```
MX# clear user Nin lockout
success: change accepted.
```

See Also clear user lockout on page 9-2

- **set authentication minimum-password-length** on page 9-171
- **set authentication password-restrict** on page 9-171
- **set user** on page 9-184
- **set user expire-password-in**

Syntax **clear usergroup** *group-name* **attr** *attribute-name*

group-name	Name of an existing user group.
attribute-name	Name of an attribute used to authorize all the users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 9– 9 on page 178.)

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Examples The following command removes the members of the user group from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
MX# clear usergroup cardiology attr time-of-day
success: change accepted.
```

See Also

- **clear usergroup** on page 9-159
- **set usergroup** on page 9-187
- **show aaa** on page 9-189

set accounting {admin | console}

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

Syntax **set accounting** {**admin** | **console**} {*user-glob*} {**start-stop** | **stop-only**} *method1* [*method2*] [*method3*] [*method4*]

admin	Users with administrative access to the MX switch through Telnet or Web View.
console	Users with administrative access to the MX switch through a console connection.
user-glob	Single user or set of users with administrative access or network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.) **Note:** This option does not apply if **mac** is specified. For **mac**, specify a . (See **"MAC Address Globs" on page 2–7**.)

method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on. A method can be one of the following: ❑ **local**—Stores accounting records in the local database on the MX switch. When the local accounting storage space is full, MSS overwrites older records with new ones. ❑ —Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults Accounting is disabled for all users by default.

Access Enabled.

History

Version 1.0	Command introduced
Version 3.0	**console** option added

Usage For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Examples The following command issues start-and-stop accounting records at the local MX database for administrator Natasha, when she accesses the switch using Telnet or Web View:

```
MX# set accounting admin Natasha start-stop local
success: change accepted.
```

See Also

- **clear accounting** on page 9-148
- **show accounting statistics** on page 9-198

set accounting {dot1x | mac | web | last-resort}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

Syntax **set accounting** {**dot1x** | **mac** | **web | last-resort**} {**ssid** *ssid-name* | **wired**} {*user-glob* | *mac-addr-glob*} {**start-stop** | **stop-only**} *method1* [*method2*] [*method3*] [*method4*]

dot1x	Users with network access through the MX switch who are authenticated by 802.1X.
mac	Users with network access through the MX switch who are authenticated by MAC authentication
web	Users with network access through the MX switch who are authenticated by WebAAA
ssid *ssid-name*	SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type **any**.
wired	Applies this accounting rule specifically to users who are authenticated on a wired authentication port.

Defaults

Syntax **set accounting system** *method1* [*method2*] [*method3*] [*method4*]

Defaults By default MSS does not send Accounting-On or Accounting-Off messages.

Access Enabled.

History Introduced in MSS 5.0.

Usage Use this command to configure MSS to send an Accounting-On message (Acct-Status-Type = 7) to a RADIUS server when the MX switch starts, and an Accounting-Off message (Acct-Status-Type = 8) to the RADIUS server when the MX switch is adminstratively shut down.

When you enable this command, an Accounting-On message is generated and sent to the specified server or server group. Subsequent Accounting-On messages are generated each time the MX starts. When the MX is administratively shut down, an Accounting-Off message is generated.

Defaults By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is **local**

History Introduced in MSS 1.0.

Usage You can configure different authentication methods for different groups of users. (For details, see **“User Globs, MAC Address Globs, and VLAN Globs” on page 2–7**.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local MX database and sends an authenticati

protocol Protocol used for authentication. Specify one of the following:

- **eap-md5**—Extensible Authentication Protocol (EAP) with message-digest algorithm 5. :
  - Uses challenge-response to compare hashes
  - Provides *no*

Defaults By default, authentication is unconfigured for all clients with network access through MP ports or wired authentication ports on the MX switch. Connection, authorization, and accounting are also disabled for these users.

Bonded authentication is disabled by default.

Access Enabled.

History

set authentication mac

Configures authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

Syntax **set authentication mac** {**ssid** *ssid-name* | **wired**} *mac-address-glob method1* [*method2*] [*method3*] [*method4*]

Defaults By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default. When using RADIUS for authentication, the default password for MAC and last-resort users is .

Access Enabled.

History

Usage You can configure different authentication methods for different groups of MAC addresses by "globbing." (For details, see **"User Globs, MAC Address Globs, and VLAN Globs" on page 2–7**.)

If you specify multiple authentication methods in the **set authentication mac** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local MX database and sends an authentication request to the RADIUS server group.

If the MX configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to

set authentication minimum-password-length

Specifies the minimum allowable length for user passwords.

Syntax **set authentication minimum-password-length** *length*

Defaults By default, there is no minimum length for user passwords.

Access Enabled.

History Introduced in MSS 6.0.

Usage Use this command to specify the minimum length for user passwords. When this command is configured, you cannot configure a password shorter than the specified length.

When you enable this command, MSS evaluates the passwords configured on the MX switch and displays a list of users whose password does not meet the minimum length restriction.

Examples To set the minimum length for user passwords at 7 characters, type the following command:

```
MX# set authentication minimum-password-length 7
warning: the following users have passwords that are shorter than the minimum password
length -
 dan
 admin
 user2
 goofball
success: change accepted.
```

See Also

- **clear user lockout** on page 9-158
- **set authentication minimum-password-length** on page 9-171
- **set user** on page 9-184

set authentication password-restrict

Activates password restrictions for network and administrative users.

Syntax **set authentication password-restrict** {**enable** | **disable**}

Defaults By default the password restrictions are disabled.

Access Enabled.

- When a user changes his or her password, at least 4 characters must be different from the previous password.

When you enable the password restrictions, MSS evaluates the passwords configured on the MX switch and displays a list of users whose password does not meet the restriction on length and character types.

Examples To enable password restrictions on the MX switch, type the following command:

```
MX# set authentication password-restrict enable
warning: the following users have passwords that do not have atleast 2 each of upper-case
letters, lower-case letters, numbers and special characters -
 dan
 admin
 user1
 user2
 goofball
 dang
success: change accepted.
```

See Also

- **set authentication minimum-password-length** on page 9-171
- **set authentication max-attempts** on page 9-170
- **clear user lockout** on page 9-158

set authentication proxy

Configures a proxy authentication rule for wireless users on a third-party AP.

Syntax **set authentication proxy ssid** *ssid-name user-glob radius-server-group*

ssid *ssid-name*	SSID name to which this authentication rule applies.
user-glob	A single user or a set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.)
radius-server-group	A group of RADIUS servers

Defaults None.

Access Enabled.

History Introduced in MSS 4.0.

Usage AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the .

Examples The following command configures a proxy authentication rule that matches on all usernames associated with SSID . MSS uses RADIUS server group to proxy RADIUS requests and hence to authenticate and authorize the users.

```
MX# set authentication proxy ssid mycorp ** srvrgrp1
```

See Also

- **clear authentication proxy** on page 9-152
- **set radius proxy client** on page 17-429

- **set radius proxy port** on page 17-429

set authentication web

Configures an authentication rule that allows a user to log into the network using a web page served by the MX. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax **set authentication web** {**ssid** *ssid-name* | **wired**} *user-glob* *method1* [*method2*] [*method3*] [*method4*]

user-glob	A single user or a set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.)
ssid *ssid-name*	SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
wired	Applies this authentication rule specifically to users connected to a wired authentication port.
method1 *method2* *method3* *method4*	At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following: ❑ **local**—Uses the local database of usernames and user groups on the MX switch for authentication. ❑ —Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. RADIUS servers cannot be used with the EAP-TLS protocol. For more information, see "Usage."

Defaults By default, authentication is unconfigured for all clients with network access through MP ports or wired authentication ports on the MX switch. Connection, authorization, and accounting are also disabled for these users.

Access Enabled.

History Introduced in MSS 3.0.

Usage You can configure different authentication methods for different groups of users by "globbing." (For details, see **"User Globs" on page 2–7**.)

You can configure a rule either for wireless access to an SSID, or for wired access through an MX wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

If you specify multiple authentication methods in the **set authentication web** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local MX database and sends an authentication request to the server group.

MSS uses a WebAAA rule only under the following conditions:

- The client is not denied access by 802.1X or does not support 802.1X.

- The client MAC address does not match a MAC authentication rule.
- The fallthru type is

ssid *operator ssid-name*	SSID with which the user is associated. The must be **eq**, which applies the location policy rule to all users associated with the SSID Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.
time-of-day *operator time-of-day*	Time of day that the user is allowed or denied access to the wireless network. ❑ **eq**—Defines a specific timeframe ❑ **neq**—Defines any other time than the specified timeframe.
vlan *operator vlan-glob*	VLAN-Name attribute assigned by AAA and condition that determines if the location policy rule applies. Replace with one of the following operands: ❑ **eq**—Applies the location policy rule to all users assigned VLAN names matching ❑ **neq**—Applies the location policy rule to all users assigned VLAN names matching For , specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an sign (@) or a period (.). (For details, see **"VLAN Globs" on**

Defaults By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

Access Enabled.

History

Usage Only a single location policy is allowed per MX switch. The location policy can contain up to 150 rules. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the **clear location policy** command.

Conditions within a rule are AND'ed. All conditions in the rule must match in order for MSS to take the specified action. If the location policy contains multiple rules, MSS compares the user information to the rules one at a time, in the order the rules appear in the MX configuration file, beginning with the rule at the top of the list. MSS continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use **before** and **modify** in the **set location policy** command, and the **clear location policy** command.

When applying security ACLs:

- Use **inacl** to filter traffic that enters the MX from users via an MP access port or wired authentication port, or from the network via a network port.
- Use **outacl** to filter traffic sent from the switch to users via an MP access port or wired authentication port, or from the network via a network port.
- You can optionally add the suffixes **.in** and **.out** to and so that they match the names of security ACLs stored in the local MX database.

Examples The following command denies network access to all users at *.thout8 to

Syntax **set mac-user** *mac-address-glob*[**group** *group-name*]

mac-addr-glob	. Allows a group of MAC devices to authenticate, such as a group of VoIP phones. Ony ine asterisk is allowed and it must be the last character. The most specific format overrides other formats. For instance, 00:11:30:21:ab:cd overrides an entry of 00:11:30:*.
group-name	Name of an existing MAC user group.

Defaults None.

Access Enabled.

History

MSS Version 1.0	Introduced command
MSS Version 6.2	MAC glob introduced.

Usage MSS does not require MAC users to belong to user groups.

Users authenticated by MAC address are authenticated only for network access through the MX. MSS does not support passwords for MAC users.

Examples The following command creates a user profile for a user at MAC address 01:02:03:04:05:* and assigns the user to the user group:

```
MX# set mac-user 01:02:03:04:05:* group eastcoasters
success: change accepted.
```

See Also

- **clear mac-user** on page 9-154
- **show aaa** on page 9-189

set mac-user attr

Assigns an authorization attribute in the local database on the MX to a user authenticating with a MAC address.

(To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax **set mac-user** *mac-address-glob* **attr** *attribute-name value*

mac-address-glob	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
attribute-name value	Name and value of an attribute used to authorize the MAC user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to local users, see Table 9– 9 on page 178.

Defaults None.

Access Enabled.

History

MSS Version 1.0	Command introduced
MSS Version 1.1	Authorization attributes **encryption-type** and **time-of-day** added
MSS Version 3.0	Authorization attributes **end-date**, **ssid**, **start-date**, and **url** added
MSS Version 5.0	Authorization attribute **acct-interim-interval** added

Usage To change the value of an attribute, enter **set mac-user attr** with the new value. To delete an attribute, use **clear mac-user attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is earlier than the start-date configured for the MAC user group for the user, the MAC user network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group start date.

ssid (network access mode only)	SSID accessible by the user after authentication.	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to Trapeze radios in the Mobility Domain.
start-date	Date and time at which the user becomes eligible to access the network. MSS does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).	Date and time, in the following format: YY/MM/DD-HH:MM You can use **start-date** alone or with **end-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.
time-of-day (network access mode only)	Day(s) and time(s) during which the user is permitted to log into the network. After authorization, the user session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter. **Note:** Time-Of-Day is a Trapeze vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 4.	One of the following: ❑ **never**—Access is always denied. ❑ **any**—Access is always allowed. ❑ **al**—Access is always allowed. ❑ One or more ranges of values that consist of one of the following day designations (required), and a time range in 4-digit 24-hour format (optional): • **mo**—Monday • **tu**—Tuesday • **we**—Wednesday • **th**—Thursday • **fr**—Friday • **sa**—Saturday • **su**—Sunday • **wk**—Any day between Monday and Friday Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (|). Do not use spaces. The maximum number of characters is 253. For example, to allow access only on Tuesdays and Thursdays between 10 a.m. and 4 p.m., specify the following: **time-of-day tu1000-1600,th1000-1600**
time-of-day (network access mode only)		

url (network access eyde only)	URL to redirect the user after successful WebAAA.	Web URL, in standard format. For example: http://www.example.com **Note:** You must include the portion. You can dynamically include any of the variables in the URL string:

Examples The following command assigns input access control list (ACL) to filter packets from a user at MAC address 01:02:03:04:05:06:

```
MX# set mac-user 01:02:03:04:05:06 attr filter-id acl-03.in
success: change accepted.
```

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

```
MX# set mac-user 06:05:04:03:02:01 attr time-of-day
   mo1900-1159,tu0000-0700,we1900-1159,th0000-0700
success: change accepted.
```

See Also

- **clear mac-user attr** on page 9-154
- **show aaa** on page 9-189

set mac-usergroup attr

Creates a user group in the local database on the MX for users authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax **set mac-usergroup** *group-name* **attr** *attribute-name value*

group-name	Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character.
attribute-name value	Name and value of an attribute used to authorize all MAC users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 9– 9 on page 178.)

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Usage To change the value of an attribute, enter **set mac-usergroup attr** with the new value. To delete an attribute, use **clear mac-usergroup attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group of the MAC user, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is earlier than the start-date configured for the MAC user group, the MAC user network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group start date.

Examples The following command creates the MAC user group and assigns the group members to VLAN :

```
MX# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.
```

See Also

- **clear mac-usergroup attr** on page 9-156
- **show aaa** on page 9-189

set mobility-profile

Creates a Mobility Profile and specifies the MP and/or wired authentication ports on the MX through which any user assigned to the profile is allowed access.

Syntax **set mobility-profile name** *name*
{**port** {**none** | **all** | *port-list*}} | {**ap** {**none** | **all** | *apnum*}}

name	Name of the Mobility Profile. Specify up to 32 alphanumeric characters, with no spaces.
none	Prevents any user to whom this profile is assigned from accessing any MP access point or wired authentication port on the MX switch.
all	Allows any user to whom this profile is assigned to access all MP access ports and wired authentication port on the MX switch.

port-list	List of MP access ports or wired authentication ports through which any user assigned this profile is allowed access. The same port can be used in multi1 Tin ty Profile port lists.
ap-num	List of MP connections through which any user assigned this profile is allowed access. The same MP can be used in multiple Mobility Profile port lists.

Defaults No default Mobility Profile exists on the MX. If you do not assign Mobility Profile attributes, all users have access through all ports, unless denied access by other AAA servers or by access control lists (ACLs).

Access Enabled.

History

Version 1.0	Command introduced
Version 2.0	Option **dap** added for Distributed MPs

Usage To assign a Mobility Profile to a user or group, specify it as an authorization attribute in one of the following commands:

- **set user attr mobility-profile**
- **set usergroup attr mobility-profile**
- **set mac-user attr mobility-profile**
- **set mac-usergroup attr mobility-profile**

To enable the use of the Mobility Profile feature on the MX switch, use the **set mobility-profile mode** command.

When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local MX database or RADIUS server when no Mobility Profile of that name exists on the MX.

To change the ports in a profile, use **set mobility-profile** again with the updated port list.

Examples The following commands create the Mobility Profile , which restricts user access to port 12; enable the Mobility Profile feature on the MX switch; and assign the Mobility Profile to user .

```
MX# set mobility-profile name magnolia port 12
success: change accepted.

MX# set mobility-profile mode enable
success: change accepted.

MX# set user Jose attr mobility-profile magnolia
success: change accepted.
```

The following command adds port 13 to the Mobility Profile (which is already assigned to port 12):

```
MX# set mobility-profile name magnolia port 12-13
success: change accepted.
```

See Also

- **clear mobility-profile** on page 9-156
- **set mac-user attr** on page 9-177
- **set mac-usergroup attr** on page 9-182

- **set mobility-profile mode** on page 9-184
- **set user attr** on page 9-185
- **set usergroup** on page 9-187
- **show mobility-profile** on page 9-200

set mobility-profile mode

Enables or disables the Mobility Profile feature on the MX switch.

When the Mobility Profile feature is

Syntax **set mobility-profile mode** {**enable** | **disable**}

Defaults The Mobility Profile feature is disabled by default.

Access Enabled.

History Introduced in MSS 1.0.

Examples To enable the use of the Mobility Profile feature, type the following command:

```
MX# set mobility-profile mode enable
success: change accepted.
```

See Also

- **clear mobility-profile** on page 9-156
- **set mobility-profile** on page 9-182
- **show mobility-profile** on page 9-200

set user

Configures a user profile in the local database on the MX for a user with a password.

(To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax **set user** *username* **password** [**encrypted**] *string*

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Usage The **show config** command shows the **encrypted** option with this command, even when you omit the option. The **encrypted** option appears in the configuration because MSS automatically encrypts the password when you create the user (unless you use the **encrypted** option when you enter the password).

Although MSS allows you to configure a user password for the special "last-resort" guest user, the password has no effect. Last-resort users can never access an MX in administrative mode and never require a password.

The only valid username of the form is . The user allows last-resort access on a wired authentication port.

Examples The following command creates a user profile for user Nin in the local database, and assigns the password :

```
MX# set user Nin password goody
success: User Nin created
```

The following command assigns the password to the **admin** user:

```
MX# set user admin password chey3nne
success: User admin created
```

The following command changes the password for Nin from to

```
MX# set user Nin password 29Jan04
```

See Also

- **clear user** on page 9-157
- **show aaa** on page 9-189

set user attr

Configures an authorization attribute in the local database on the MX for a user with a password.

(To assign authorization attrib

Usage To change the value of an attg a12 540 -6ea enter/TT6 1 Tf89.96 0113.0846 1021Tc-8029 Tw02Toset user/

set user group

Usage To change the value of an attribute, enter **set usergroup attr** with the new value. To delete an attribute, use **clear usergroup attr**.

To a user to a group, user the command **set user group**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user belongs, the attributes assigned to the individual user take

set web-portal

Globally enables or disables WebAAA on an MX.

Syntax show mac-user [*mac-glob*|verbose]

mac-glob	Displays MAC addresses based on the MAC format
verbose	Displays all MAC user information

Defaults None

Access Enabled

History

Version 6.2	Command introduced

Examples To display all MAC users, type the following command:

```
MX# show mac-user
```

```
MX# show mac-user [<mac-glob>|verbose]

MAC               Group        VLAN
----------------  --------     -------
00:11:11:21:11:1  Guests       insecure
2
00:11:11:21:11:*  Guests       red

MX# show mac-user 00:11:11:21:11:12

MAC               Group        VLAN
----------------  --------     -------
00:11:11:21:11:1  Guests       insecure
2
```

```
MX# show mac-user verbose

MAC:                          00:11:11:21:12
Group:                        Guests
VLAN                          insecure
Other attributes:
ssid:                         trapeze
end-date:                     01/08/23-12:00
idle-timeout:                 120
acct-interim-interval:        180
MAC:                          00:11:11:21:*
Group:                        Guests
VLAN                          insecure
Other attributes:
ssid:                         trapeze
end-date:                     01/08/23-12:00
idle-timeout:                 120
acct-interim-interval:        180
```

```
MX# show mac-user 00:11:11:21:11* verbose

MAC:                          00:11:11:21:*
Group:                        Guests
VLAN                          insecure
Other attributes:
ssid:                         trapeze
end-date:                     01/08/23-12:00
idle-timeout:                 120
acct-interim-interval:        180
```

Table 9– 14 describes the fields that can appear in the **show mac-user** output.

MAC	MAC address
Group	Member of a configured group
VLAN	Current VLAN of the MAC user
Other attributes	Other AAA attributes
ssid	Current SSID configured for the MAC user
end-date	The expiration date fo the MAC user
idle-timeout	Number of seconds the user is idle before the connection is lost.
acct-interim-interval	Interval in seconds between accounting updates, if start-stop accounting mode is enabled.

show mac-usergroup

Displays summary status for all MAC usergroups or verbose status for a specific MAC usergroup.

Syntax show mac-usergroup [*mac-ug-name*|verbose]

mac-ug-name	Configured usergroup name
verbose	Detailed information about a MAC usergroup

Defaults None

Access Enabled

History Introduced in MSS Version 6.2

Examples The following command displays information about MAC usergroups:

```
MX# show mac-usergroup [<mac-ug-name>|verbose]

                        Users Mapped            Other
MAC Usergroup           to Group        VLAN    Attr. of
------------------      --------------  ------  Group
Admin                   0               red     3
Guests                  2               insecure 4

MX# show mac-usergroup Guests

MAC Usergroup:                  Guests2
VLAN:                           blue
Other attributes:
ssid:                           trapeze
end-date:                       01/08/23-12:00
idle-timeout:                   120
acct-interim-interval:          180

MAC users in this group:

MAC             VLAN
------------    --------
00:11:11:21:11:  insecure
12
00:11:11:21:11:  red
*

MX# show mac-usergroup Admin

MAC Usergroup:                  Admin
VLAN:                           red
Other attributes:
ssid:                           trapeze
idle-timeout:                   120
acct-interim-interval:          180

No MAC users in this group.
```

Table 9– 11 describes the fields that can appear in the **show mac-usergroup** output.

MAC Usergroup	List of the configured MC Usergroups
Users Mapped to Group	The number of users configured in each group
VLAN	The VLAN configured for a usergroup
Other attr of the group	The number of configured attributes for the group

```
MX# show user verbose

User name:                      johndoe
Status:                         disabled
Password:                       iforgot(encypted)
Group:                          Admin
VLAN:                           red
Password-expires-in:            12 days
Other attributes:
ssid:                           trapeze
end-date:                       01/08/23-12:00
idle-timeout:                   120
acct-interim-interval:          180
User name:                      johnsmith
Status:                         enabled
Password:                       iforgot2(encypted)
Group:                          Admin
VLAN:                           red
Password-expires-in:            12 days
Other attributes:
None
User name:                      guest_access
Status:                         disabled
Password:                       iforgot3(encypted)
Group:                          Admin
VLAN:                           red
Password-expires-in:            5 days
Other attributes:
ssid:                           trapeze1
end-date:                       01/08/20-9:00
idle-timeout:                   100
acct-interim-interval:          600
```

```
MX# show user *john* verbose

User name:                      johndoe
Status:                         disabled
Password:                       iforgot(encypted)
Group:                          Admin
VLAN:                           red
Password-expires-in:            12 days
Other attributes:
ssid:                           trapeze
end-date:                       01/08/23-12:00
```

```
idle-timeout:                   120
acct-interim-interval:          180
User name:                      johnsmith
Status:                         enabled
Password:                       iforgot2(encypted)
Group:                          Admin
VLAN:                           red
Password-expires-in:            12 days
Other attributes:
None
```

Table 9– 12 decscribes the fields tht can appear in **show user** output.

User Name	Name configured for a user on the MX.
Status	Current condition of the client: ❑ Enabled— ❑ Disabled
Password	Displays a user's password and if it is encrypted or not.
Group	Name of a usergroup if configured
VLAN	The name of the VLAN configured for the user.
Password-expires-in	The length of time, in days, before a user's password expires.
Other attributes	Additional attributes configured for user.

show usergroup

Displays summary status for a single user group or all user groups.

Syntax `show usergroup` *ug-name*

Defaults None

Access Enabled

History Command introduced in MSS 6.2

Examples

end-date	The date and time that the usergroup is no longer valid.
idle-timeout	The length of time, in seconds, that a user can be idle before logging out of the network.
acct-interm-interval	Interval in seconds between accounting updates, if start-stop accounting mode is enabled
Users in this group:	All users configured in the usergroup
User Name	Configured user names in this group
VLAN	Assigned VLAN for each user.

MAC	MAC address of the user
Group	The user group for the MAC-user
VLAN	The VLAN assigned to the mac-user

See Also

- **set accounting {admin | console}** on page 9-160
- **set authentication admin** on page 9-163
- **set authentication console** on page 9-165
- **set authentication dot1x** on page 9-166
- **set authentication mac** on page 9-169
- **set authentication web** on page 9-173

show accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the MX.

(To display RADIUS accounting records, see the documentation for your RADIUS server.)

Syntax **show accounting statistics**

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 4.2	Formatting of output enhanced for readability

Examples To display the locally stored accounting records, type the following command:

```
MX# show accounting statistics
Dec 14 00:39:48
Acct-Status-Type=STOP
Acct-Authentic=0
```

```
Acct-Multi-Session-Id=SESS-3-01f82f-520236-24bb1223
Acct-Session-Id=SESS-3-01f82f-520236-24bb1223
User-Name=vineet
AAA_ACCT_SVC_ATTR=2
Acct-Session-Time=551
Event-Timestamp=1134520788
Acct-Output-Octets=3204
Acct-Input-Octets=1691
Acct-Output-Packets=20
Acct-Input-Packets=19
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Dec 14 00:39:53
Acct-Status-Type=START
Acct-Authentic=0
User-Name=vineet
Acct-Multi-Session-Id=SESS-4-01f82f-520793-bd779517
Acct-Session-Id=SESS-4-01f82f-520793-bd779517
Event-Timestamp=1134520793
AAA_ACCT_SVC_ATTR=2
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x
```

Table 9– 15 describes the fields that can appear in **show accounting statistics** output.

Date and time	Date and time of the accounting record.
Acct-Status-Type	Type of accounting record: ❑ START ❑ STOP ❑ UPDATE
Acct-Authentic	Location where the user was authenticated (if authentication took place) for the session: ❑ 1—RADIUS server ❑ 2—Local MX database
User-Name	Username of a user with a password.
Acct-Multi-Session-Id	Unique accounting ID for multiple related sessions in a log file.
AAA_TTY_ATTR	For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number.
Event-Timestamp	Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.)
Acct-Session-Time	Number of seconds that the session has been online.
Acct-Output-Octets	Number of octets the MX sent during the session.
Acct-Input-Octets	Number of octets the MX received during the session.

Acct-Output-Packets	Number of packets the MX sent during the session.
Acct-Input-Packets	Number of packets the MX received during the session.
Vlan-Name	Name of the client VLAN.
Calling-Station-Id	MAC address of the supplicant (client).
Nas-Port-Id	Number of the port and radio on the MP through which the session was conducted.

See Also

- **clear accounting** on page 9-148
- **set accounting {admin | console}** on page 9-160
- **show aaa** on page 9-189

show location policy

Displays the list of location policy rules that make up the location policy on an MX.

Syntax **show location policy**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.1.

Examples The following command displays the list of location policy rules in the location policy on an MX :

```
MX show location policy
Id Clauses
-----------------------------------------------------------------
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.wodefirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com
```

See Also

- **clear location policy** on page 9-153
- **set location policy** on page 9-174

show mobility-profile

Displays the named Mobility Profile. If you do not specify a Mobility Profile name, this command shows all Mobility Profile names and port lists on the MX.

Syntax **show mobility-profile** [*name*]

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 2.0	Port type description added: ❑ AP—MP access port ❑ DAP—Distributed MP connection

Examples The following command displays the Mobility Profile :

```
MX# show mobility-profile magnolia
Mobility Profiles
Name                Ports
========================
magnolia         AP 12
```

See Also

- **clear mobility-profile** on page 9-156
- **set mobility-profile** on page 9-182

Use Mobility Domain commands to configure and manage Mobility Domain groups.

A Mobility Domain is a system of MXs and MPs working together to support a roaming user (client). One MX acts as a seed MX, which maintains and distributes a list of IP addresses of the domain members.

Smart Cluster is a network resiliency feature added in MSS 7.0. It has the following features:

- Centralized configuration of MXs and MPs.
- Autodistribution of configuration parameters to MPs.
- "Hitless" failover on the network if an MX is unavailable.
- Automatic load balancing of MPs across any MXs in the cluster.

The number of MPs supported on a cluster member is limited to the number supported on an MX. It is recommended to use larger capacity MXs, such as MX-200s, MS-216s, or MX-2800s in your configuration to obtain the maximum benefits of cluster configuration.

Trapeze Networks recommends that you run the same MSS version on all the MX switches in a Mobility Domain and Smart Cluster.

This chapter presents Mobility Domain commands alphabetically. Use the following table to locate commands in this chapter based on their use.

clear domain security

Disables MX-MX security.

Syntax `clear domain security`

Defaults

Usage This command has no effect if the MX member is not configured as part of a Mobility Domain or the current MX is not the seed.

Examples The following command clears a Mobility Domain member with the IP address 192.168.0.1:

```
MX-20# clear mobility-domain member 192.168.0.1
```

See Also **set mobility-domain member** on page 10-206

Syntax **set domain security** {**none** | **required**}

none	MX-MX security is disabled.
required	MX-MX security is enabled.

Defaults The default is **none**. (MX-MX security is disabled.)

Access Enabled.

History Introduced in MSS 5.0.

Usage The setting must be the same (**none** or **required**) on all switches, the seed and all members, in the Mobility Domain.

The **set domain security none** command is equivalent to the **clear domain security** command.

Examples The following command enables MX-MX security on an MX:

```
MX# set domain security required
success: change accepted.
```

set mobility-domain member

On the seed MX, adds a member to the list of Mobility Domain members. If the current MX is not configured as a seed, this command is rejected.

Syntax **set mobility-domain member** *ip-addr* **key** *hex-bytes*

ip-addr	IP address of the Mobility Domain member in dotted decimal notation.
key *hex-bytes*	Fingerprint of the public key to use for MX-MX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: `00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff`

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 5.0	Option **key** added.

Usage This command must be entered from the seed MX.

Examples The following commands add three MX switches with the IP addresses 192.168.1.8, 192.168.1.9, and 192.168.1.10 as members of a Mobility Domain with a seed as the current MX:

```
MX# set mobility-domain member 192.168.1.8
success: change accepted.

MX# set mobility-domain member 192.168.1.9
success: change accepted.

MX# set mobility-domain member 192.168.1.10
success: change accepted.
```

See Also

- **clear mobility-domain member** on page 10-204

- **set mobility-domain mode seed domain-name** on page 10-209
- **show mobility-domain config** on page 10-210

set mobility-domain mode member secondary-seed-ip

Sets the IP address of the secondary seed MX on a nonseed MX.

Syntax **set mobility-domain mode member secondary-seed-ip** *secondary-seed-ip-addr* **key** *hex-bytes*

secondary-seed-ip-addr	IP address of the secondary seed, in dotted decimal notation.
key *hex-bytes*	Fingerprint of the public key to use for MX-MX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: `00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff`

Defaults None.

Access Enabled.

History Introduced in MSS 1.0

Examples The following command sets the current MX as a nonseed member of the Mobility Domain whose secondary seed has the IP address 192.168.1.8:

```
MX# set mobility-domain mode member seed-ip 192.168.1.8
mode is: member
seed IP is: 192.168.1.8
```

See Also

- **clear mobility-domain** on page 10-204
- **show mobility-domain config** on page 10-210

set mobility-domain mode member seed-ip

On a nonseed MX, sets the IP address of the seed MX. This command is used on a member MX to configure it as a member. If the MX is currently part of another Mobility Domain or using another seed, this command overwrites that configuration.

Syntax **set mobility-domain mode member seed-ip** *ip-addr* **key** *hex-bytes*

ip-addr	IP address of the Mobility Domain member, in dotted decimal notation.
key *hex-bytes*	Fingerprint of the public key to use for MX-MX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: `00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff`

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 5.0	Option **key** added.

show cluster ap

Displays all MPs configured on cluster member.

Syntax **show cluster ap**

Defaults None

Access Enabled

History Introduced in MSS 7.0.

Examples The following command displays the MPs configured on a cluster member:

```
MX# show cluster ap
Primary AP Manager(PAM) and Secondary AP manager(SAM) List:
Flags:L - Cluster Load Balancing; C - Connection Wait; S - Session setup Wait

 AP     PAM MX IP        SAM MX IP    AP connected to PAM  AP connected to SAM
---- --------------  -------------- ------------------  ------------------
   3  192.168.254.85   192.168.254.83                YES                 YES
  12  192.168.254.83   192.168.254.85                YES                 YES
   6  192.168.254.85   192.168.254.83                YES                 YES
  15  192.168.254.85   192.168.254.83                YES                 YES
   9  192.168.254.85   192.168.254.83                YES                 YES
  14  192.168.254.83   192.168.254.85                YES                 YES
  10  192.168.254.83   192.168.254.85                YES                 YES
   4  192.168.254.85   192.168.254.83                YES                 YES
   5  192.168.254.85   192.168.254.83                YES                 YES
   1  192.168.254.85   192.168.254.83                YES                 YES
   2  192.168.254.85   192.168.254.83                YES                 YES
   8  192.168.254.83   192.168.254.85                YES                 YES
   7  192.168.254.85   192.168.254.83                YES                 YES
```

show mobility-domain config

This command was deprecated in MSS 7.0.

show mobility-domain

On the seed MX, displays the Mobility Domain status and members.

Syntax **show mobility-domain**

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 7.0	Updated with cluster information

Examples To display Mobility Domain status, type the following command:

```
MX# show mobility-domain
Mobility Domain name:  Mobility1
Flags: u = up[2], d = down[2], c = cluster enabled[1], p = primary seed,
       s = secondary seed, m = member, a = active seed, y = syncing,
       w = waiting to sync, n = sync completed, f = sync failed
Member           Flags  Model     Version     NoAPs  APLic
---------------  -----  --------  ----------  -----  -----
10.8.107.1       upacn  MX-20     7.0.1.0         0     40
10.2.28.71       dm---  Unknown   Unknown         0      0
10.2.28.72       dm---  Unknown   Unknown         0      0
10.2.28.74       um---  MX-20     7.0.1.0         0     40
```

Table 10– 1 describes the fields in the display.

Mobility Domain name	Name of the Mobility Domain
Flags	Indicates various states of the Mobility Domain members. ❑ u = up ❑ d = down ❑ c = cluster enabled ❑ p = primary seed ❑ s = secondary seed ❑ m = member ❑ a = active seed ❑ y = syncing ❑ w = waiting to sync ❑ n = sync completed ❑ f = sync failed
Member	IP addresses of the seed MX and members in the Mobility Domain
Flags	State of the MX in the Mobility Domain: Letters indicate which flags are present.
Model	Model of MX switch
Version	MSS version running on the MX.
NoAPs	Number of APs per MX
APLic	Number of AP licensed per MX.

See Also

- **clear mobility-domain** on page 10-204
- **set mobility-domain member** on page 10-206
- **set mobility-domain mode member seed-ip** on page 10-207

Use Network Domain commands to configure and manage Network Domain groups.

A Network Domain is a group of geographically dispersed Mobility Domains that share information over a WAN link. This shared information allows a user configured on an MX in one Mobility Domain to establish connectivity with an MX in another Mobility Domain in the same Network Domain. The MX forwards the user traffic by creating a VLAN tunnel to an MX in the remote Mobility Domain.

In a Network Domain, one or more MX switches serve as a seed switch. At least one of the Network Domain seeds maintains a connection with each of the member MX switches in the Network Domain. The Network Domain seeds share information about the VLANs configured on their members, so that all the Network Domain seeds have a common database of VLAN information.

This chapter presents Network Domain commands alphabetically. Use the following table to locate commands in this chapter based on their use.

clear network-domain

Clears all Network Domain configuration and information from an MX, regardless of whether the MX is a seed or a member of a Network Domain.

Syntax `clear network-domain`

Defaults None.

Access Enabled.

History Introduced in MSS 4.1.

Usage This command has no effect if the MX is not configured as part of a Network Domain.

Examples To clear a Network Domain from an MX within the domain**,** type the following command:

```
MX-20# clear network-domain
This will clear all network-domain configuration. Would you like to continue? (y/n) [n] y
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 11-215
-

- **set network-domain mode seed domain-name**

```
success: change accepted.
```

See Also **set network-domain peer** on page 11-216

clear network-domain seed-ip

Removes the specified Network Domain seed from the MX configuration. When you enter this command, the Network Domain TCP connections between the MX switch and the specified Network Domain seed are closed.

Syntax **clear network-domain seed-ip** *ip-addr*

Defaults None.

```
success: change accepted.
```

The following command sets the MX as a member of a Network Domain with a seed that has the IP address 192.168.9.254 and sets the affinity for that seed to 7. If the MX specifies other Network Domain seeds, and they are configured with the default affinity of 5, then 192.168.9.254 becomes the primary Network Domain seed for the MX.

```
MX# set network-domain mode member seed-ip 192.168.9.254 affinity 7
success: change accepted.
```

See Also

- **clear network-domain** on page 11-213
- **show network-domain** on page 11-217

set network-domain peer

On a Network Domain seed, configures one or more MX switches as redundant Network Domain seeds. The seeds in a Network Domain share information about the VLANs configured on the member devices, so that all the Network Domain seeds have the same database of VLAN information.

Syntax **set network-domain peer** *ip-addr*

ip-addr	IP address of the Network Domain seed to specify as a peer, in dotted decimal notation.

Defaults None.

Access Enabled.

History Introduced in MSS 4.1.

Usage This command must be entered on an MX configured as a Network Domain seed.

Examples The following command sets the MX with IP address 192.168.9.254 as a peer of this Network Domain seed:

```
MX# set network-domain peer 192.168.9.254
success: change accepted.
```

See Also

- **clear network-domain** on page 11-213
- **show network-domain** on page 11-217

set network-domain mode seed domain-name

Creates a Network Domain by setting the current MX as a seed device and naming the Network Domain.

Syntax **set network-domain mode seed domain-name** *net-domain-name*

net-domain-name	Name of the Network Domain. Specify between 1 and 16 characters with no spaces.

Defaults None.

Access Enabled.

History Introduced in MSS 4.1.

Use MP access point commands to configure and manage MP access points. Be sure to do the following before using the commands:

- Define the country-specific IEEE 802.11 regulations on the MX. (See **set system countrycode** on page 4-29.)
- Install the MP and connect it to a port on the MX. (See the or .)
-

	clear radio-profile on page 12-226
	set radio-profile service-profile on page 12-275
	show radio-profile on page 12-344
SSID Assignment	**set service-profile ssid-name** on page 12-303
	set service-profile ssid-type on page 12-304
	set service-profile beacon on page 12-284
Radio Properties	**set radio-profile active-scan** on page 12-256
	set radio-profile beacon-interval on page 12-263
	set radio-profile countermeasures on page 12-265
	set radio-profile dfs-channels on page 12-265
	set radio profile fair-queuing-weight
	set radio-profile frag-threshold on page 12-267
	set radio-profile max-rx-lifetime on page 12-268
	set radio-profile max-tx-lifetime on page 12-268
	set radio-profile preamble-length on page 12-271
	set radio-profile rts-threshold on page 12-275
Authentication and Encryption	**set service-profile attr** on page 12-281
	set service-profile auth-dot1x on page 12-282
	set service-profile auth-fallthru on page 12-283
	set service-profile web-portal-form on page 12-309
	set service-profile web-portal-acl

	set service-profile cac-mode on page 12-286
	set service-profile cac-session on page 12-286
	set service-profile static-cos on page 12-304
	set service-profile cos on page 12-289
	set service-profile use-client-dscp on page 12-307
DHCP Restrict	**set service-profile dhcp-restrict** on page 12-290
Broadcast control	**set service-profile no-broadcast** on page 12-294
Proxy ARP	**set service-profile proxy-arp** on page 12-294
Keepalives and session timers	**set service-profile idle-client-probing** on page 12-290
	set service-profile user-idle-timeout on page 12-308
	set service-profile web-portal-session-timeout on page 12-311
Sygate On-Demand (SODA)	**set service-profile soda mode** on page 12t-dif15 2ect5.066oryrtalle-timeout

Per-id(ox)-5(y-a)4

von-aertalprofile cac-session

er-i91session-timeout

Access Enabled.

History

Version 5.0 C cmand ANi5.9(esn)4(t)-roduc.

Usage Use this command to configure an MP that was converted to an AirDefense sensor to revert back to an MP. When you do this, the next time the MP is booted, it becomes a Trapeze Mobility Point.

Examples

Examples The following command causes the AirDefense sensor software file to be cleared from the configuration of MP 1:

```
MX# clear ap 1 image
success: change accepted.
```

See Also **set ap image** on page 12-241

clear ap local-switching vlan-profile

Clears the VLAN profile that had been applied to an MP to use with local switching.

Syntax **clear ap** *apnum* **local-switching vlan-profile**

Defaults None.

Access Enabled.

History

Usage A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to an MP, traffic for the VLANs specified in the VLAN profile is locally switched by the MP instead of being tunneled back to an MX.

Use this command to reset the VLAN profile used by the MP for local switching to the VLAN profile. Traffic that was locally switched because of an entry in the cleared VLAN profile is tunneled to an MX.

When clearing a VLAN profile causes traffic that was locally switched by MPs to be tunneled to an MX, the sessions of clients associated with the MPs with the VLAN profile are terminated, and the clients must re-associate with the MPs.

Examples The following command clears the VLAN profile that was applied to MP 7:

```
MX# clear ap 7 local-switching vlan-profile
success: change accepted.
```

See Also

- **set ap local-switching mode** on page 12-242
- **set ap local-switching vlan-profile** on page 12-242
- **set vlan-profile** on page 6-75

clear ap radio

Disables an MP radio and resets it to its factory default settings.

Syntax **clear ap** *apnum* **radio** {**1** | **2** | **all**}

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value between 1 and 9999.
radio 1	Radio 1 of the MP.
radio 2	Radio 2 of the MP. (This option does not apply to single-radio models.)
radio all	All radios on the MP.

Defaults The **clear ap radio** command resets the radio to the default settings listed in **Table 12– 1** and in Table 12– 3 on page 269.

antenna-location	**indoors**	Location of the radio antenna. **Note:** This parameter applies only to MP models that support external antennas.
antennatype	For most MP models, the default is **internal**. For MP-620, the default for the 802.11b/g radio is **ANT-1360-OUT**. The default for the 802.11a radio is **ANT-5360-OUT**.	

Access Enabled

History

clear ap radio load-balancing group

Removes an MP radio from a load-balancing group.

Syntax **clear ap** *apnum* **radio** {**1** | **2**} **load-balancing group**

Defaults If you reset an individual parameter, the parameter is returned to the default value listed in Table 12– 3 on page 269.

Access Enabled.

History

Usage If you specify a parameter, the setting is reset to the default value. The settings of the other pa 1 Trs are yo5.5.3(n.5.ch6(a5.5.grne6(a5.5.d4(th(e)-6 pa.6(dt)4.o 6(p)r(l)2(ofdt)4.il(r)]TJ)-4.9578 0 T-g.

soda failure-page	Resets the page loaded when a client fails the SODA agent checks. By default, the page is generated dynamically.
soda remediation-acl	Disables use of the specified remediation ACL for the service profile. When no remediation ACL is specified, a client is disconnected from the network when it fails SODA agent checks.
soda success-page	Resets the page loaded when a client passes the checks performed by the SODA agent. By default, the page is generated dynamically.
soda logout-page	Resets the page loaded when a client logs out of the network. By default, the client is disconnected from the network without loading a page.

Defaults None.

Access Enabled.

History

Version 3.0	Command introduced
Version 4.2	Options added to clear SODA parameters.

Usage If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the **clear radio-profile service-profile** command.)

Examples The following commands disable the radios using radio profile , remove service-profile from , then clear from the configuration.

```
MX# set radio-profile rp6 mode disable
MX# clear radio-profile rp6 service-profile svcprof6
success: change accepted.
MX# clear service-profile svcprof6
success: change accepted.
```

- **clear radio-profile** on page 12-226
- **set radio-profile mode** on page 12-269
- **show service-profile** on page 12-347

reset ap

Restarts an MP access point.

Syntax **reset ap** *apnum*

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value between 1 and 9999.

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced.
Version 2.0	Option **dap** added for Distributed MPs.
Version 6.0	Option **dap** removed.
Version 6.2	Added index value range of 1 to 9999.

Usage When you enter this command, the MP drops all sessions and reboots.

Restarting an MP can cause data loss for users who are currently associated with the MP.

Examples The following command resets MP 7:

```
MX# reset ap 7
This will reset specified AP devices. Would you like to continue? (y/n)y
success: rebooting ap attached to port 7
```

set ap auto

Creates a profile for automatic configuration of MPs.

Syntax `set ap auto`

Defaults None.

Access Enabled.

History

Version 4.0	Command introduced.
Version 4.2	Option **persistent** added.
Version 5.0	❑ Option **force-image-download** added. ❑ Option **radio auto-tune min-client-rate** removed. ❑ Option **radio tx-pwr** removed.
Version 6.0	❑ Option **dap** removed.

Usage **Table 12– 2** lists the configurable profile parameters and the default values. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure Distributed MPs, you must enable the profile using the **set ap auto mode enable** command.

The profile uses the default radio profile by default. You can change the profile using the **set ap auto radio radio-profile** command. You can use **set ap auto** commands to change settings for the parameters listed in **Table 12– 2**. (The commands are listed in the “See Also” section.)

MP Parameters	
bias	**high**
blink (Not shown in **show ap config** output)	**disable**
force-image-download	**disable** (NO)
group (load balancing group)	none
mode	**disabled**
persistent	none

Examples The following command creates a profile for automatic Distributed MP configuration:

```
MX# set ap auto
success: change accepted.
```

See Also

- **set ap auto mode** on page 12-230
- **set ap auto persistent**

Examples The following command enables the profile for automatic Distributed MP configuration:

```
MX# set ap auto mode enable
success: change accepted.
```

See Also

- **set ap auto** on page 12-229
- **set ap auto persistent** on page 12-231
- **set ap auto radiotype** on page 12-232
- **set ap bias** on page 12-232
- **set ap blink** on page 12-234
- **set ap group** on page 12-241
- **set ap radio auto-tune max-power** on page 12-245
- **set ap radio mode** on page 12-249
- **set ap radio radio-profile** on page 12-251
- **set ap upgrade-firmware** on page 12-253

set ap auto persistent

Converts a temporary MP configur

set ap auto radiotype

Sets the radio type for single-MP radios that use the MP configuration profile.

Syntax **set ap auto** [**radiotype** {**11a** | **11b**| **11g**}]

Defaults The default radio type for models AP2750, MP-241, and MP-341, and for the 802.11b/g

History

Usage

set ap blink

Enables or disables LED blink mode on an MP to make it easy to identify. When blink mode is enabled on MP- models, the health and radio LEDs alternately blink green and amber. When blink mode is enabled on an AP2750, the 11a LED blinks on and off. By default, blink mode is

Access Enabled.

History

Version 4.2	Command introduced.
Version 6.0	Option **dap** removed.
Version 6.2	Added the index value range of 1 to 9999.

Usage Normally, Distributed MPs use DHCP to obtain IP address information. In some installations, DHCP may not be available. In this case, you can assign static IP address information to the MP, including the MP IP address and netmask, and default gateway.

If the manually assigned IP information is incorrect, the MP uses DHCP to obtain an IP address.

Examples The following command configures MP 1 to use IP address 172.16.0.42 with a 24-bit netmask, and use 172.16.0.20 as its default gateway:

```
MX# set ap 1 boot-configuration ip 172.16.0.42 netmask 255.255.255.0 gateway 172.16.0.20
success: change accepted.
```

See Also

- **clear ap boot-configuration** on page 12-225
- **set ap boot-configuration switch** on page 12-238
- **set ap boot-configuration vlan** on page 12-239
- **show ap boot-configuration** on page 12-338

set ap boot-configuration mesh mode

Enables WLAN mesh services on the MP.

Syntax **set ap** *apnum* **boot-configuration mesh mode** {**enable**|**disable**}

ap *apnum*	Index value that identifies the MP on the MX. This can be a value from 1 to 9999.
mode {**enable**|**disable**}	Enables or disables WLAN mesh services for the MP.

Defaults Disabled.

Access Enabled.

History Introduced in MSS .

Version 6.0	Command introduced.
Version 6.2	Added index value range from 1 to 9999.

Usage Use this command to enable WLAN mesh services for an Mesh AP. Prior to deploying the Mesh AP in a final untethered location, you must connect the MP to an MX and enter this command to configure the MP for mesh services.

Examples The following command enables WLAN mesh services for MP 7:

```
MX# set ap 7 boot-configuration mesh mode enable
success: change accepted.
```

See Also

- **set ap boot-configuration mesh ssid** on page 12-237
- **set service-profile mesh** on page 12-293
- **show ap boot-configuration mesh ssid** on page 12-330
- **show service-profile mesh** on page 12-293
- **set ap boot-configuration mesh ssid** on page 12-237

set ap boot-configuration mesh psk-phrase

Specifies a preshared key (PSK) phrase that a Mesh AP uses for authentication to its Mesh Portal AP.

Syntax **set ap** *apnum* **boot-configuration mesh psk-phrase** *passphrase*

Defaults None.

Access Enabled.

History

Usage Use this command to configure the preshared key that a Mesh AP uses to authenticate to a Mesh Portal AP. You must connect the MP to an MX and enter this command to configure the MP for mesh services prior to deploying the Mesh AP in its final untethered location.

MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the MX configuration. Neither the binary number nor the passphrase is ever displayed in the configuration. To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples The following command configures MP 7 to use passphrassphthd in 485.3l56785.3l89085.3l4485.3l3<>?

Note that when the is specified, the regulatory domain of the MX and the power restrictions are copied to the MP flash memory. This prevents the Mesh AP from operating outside of regulatory limits after the AP is booted and before the AP receives a complete configuration from the MX. Consequently, it is important that the regulatory and antenna information specified on the MX actually reflects the locale where the Mesh AP is to be deployed, in order to avoid regulatory violations.

Examples The following command configures MP 7 to attempt to associate with the SSID when booted in an untethered location:

```
MX# set ap 7 boot-configuration mesh ssid wlan-mesh
success: change accepted.
```

See Also

- **set ap boot-configuration mesh mode** on page 12-235
- **set service-profile mesh** on page 12-293
- **show ap mesh-links** on page 12-330

set ap boot-configuration switch

Specifies the MX that a Distributed MP contacts and attempts to use as the boot device.

Syntax **set ap** *apnum* **boot-configuration switch** [**switch-ip** *ip-addr*] [**name** *name* **dns** *ip-addr*] [**mode** {**enable** | **disable**}]

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
switch-ip *ip-addr*	The IP address of the MX to boot the Distributed MP.
name *name*	The fully qualified domain name of the MX that the Distributed MP boots from. When both a name and a switch-ip are specified, the MP uses the name.
dns *ip-addr*	The IP address of the DNS server used to resolve the specified name of the MX.
mode {**enable** | **disable**}	Enables or disables the MP using the specified boot device.

Defaults By default MPs use the process described in “Default MP Boot Process”, in the to boot from an MX, instead of using a manually specified MX.

Access Enabled.

History

Version 4.2	Command introduced.
Version 6.0	Option **dap** removed.
Version 6.2	Added the index value range of 1 to 9999.

Usage When you specify a boot MX for a distributed MP to boot from, it boots using the process described in “MP Boot Process Using Static IP Configuration”, in the

When a static IP address is specified for a Distributed MP, there is no preconfigured DNS information or DNS name for the MX that the Distributed MP attempts to use as the boot device. If you configure a static IP address for a Distributed MP, but do not specify a boot device, then the MX must be reachable via subnet broadcast.

Examples The following command configures Distributed MP 1 to use an MX with address 172.16.0.21 as its boot device.

```
MX# set ap 1 boot-configuration switch switch-ip 172.16.0.21 mode enable
success: change accepted.
```

The following command configures Distributed MP 1 to use the MX with the name mxr2 as its boot device. The DNS server at 172.16.0.1 is used to resolve the name of the MX.

```
MX# set ap 1 boot-configuration switch name mxr2 dns 172.16.0.1 mode enable
success: change accepted.
```

See Also

- **clear ap boot-configuration** on page 12-225
- **set ap boot-configuration ip** on page 12-234
- **set ap boot-configuration vlan** on page 12-239
- **show ap boot-configuration** on page 12-338

set ap boot-configuration vlan

Specifies 802.1Q VLAN tagging information for a Distributed MP.

Syntax **set ap** *apnum* **boot-configuration vlan vlan-tag** *tag-value* [**mode** {**enable** | **disable**}]

Syntax **set ap** *apnum* **boot-configuration vlan mode** {**enable** | **disable**}

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
vlan-tag *tag-value*	The VLAN tag value. You can specify a number from 1 – 4093.
mode {**enable** | **disable**}	Enables or disables use of the specified VLAN tag on the Distributed MP.

Defaults None.

Access Enabled.

History

Version 4.2	Command introduced.
Version 6.0	Option **dap** removed.
Version 6.2	Added the index value range of 1 to 9999.

Usage When this command is configured, all Ethernet frames emitted from the Distributed MP are formatted with an 802.1Q tag with a specified VLAN number. Frames not tagged for this value and sent to the Distributed MP are ignored.

Examples The following command configures Distributed MP 1 to use VLAN tag 100:

```
MX# set ap 1 boot-configuration vlan vlan-tag 100 mode enable
success: change accepted.
```

See Also

- **clear ap boot-configuration** on page 12-225
- **set ap boot-configuration ip** on page 12-234
- **show ap boot-configuration** on page 12-338

set ap fingerprint

Verifies an MP fingerprint on an MX. If MP-MX security is required by an MX, an MP can establish a management session with the MX only if you have verified the MP identity by verifying the fingerprint on the MX.

Syntax **set ap** *apnum* **fingerprint** *fingerprint*

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
fingerprint	The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the MP.

Defaults None.

Access Enabled.

History

Version 4.0	Introduced command.
Version 6.0	Option **dap** removed.
Version 6.2	Added the index value range of 1 to 9999.

Usage MPs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the MP, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa
```

If an MP is already installed and operating, you can use the **show ap status** command to display the fingerprint. The **show ap config** command lists the MP fingerprint only if the fingerprint has been verified in MSS. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

Examples The following example verifies the fingerprint for Distributed MP 8:

```
MX# set ap 8 fingerprint b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

See Also

- **set ap security** on page 12-252
- **show ap config radio** on page 12-320
- **show ap status** on page 12-331

set ap force-image-download

Configures an MP to download a software image from the MX instead of loading the locally stored image on the MP.

Syntax **set ap auto force-image-download** {**enable** | **disable**}

ap auto	Configures forced image download for the MP configuration profile. (See **set ap auto** on page 12-229.)

force-image-download enable	Enables forced image download.
force-image-download disable	Disables forced image download.

Defaults Forced image download is disabled by default.

Access Enabled.

History

Version 5.0	Command introduced.
Version 6.0	Option **dap** removed.

Usage A change to the forced image download option takes place the next time the MP is restarted.

Even when forced image download is disabled (the default), the MP still checks with the MX to verify that the MP has the latest image, and to verify that the MX is running MSS Version 5.0 or later.

The MP loads a local image only if the MX is running MSS Version 5.0 or later and does not have a different MP image than the one in the MP local storage. If the MX is not running MSS Version 5.0 or later, or the MX has a different version of the MP image than the version in the MP local storage, the MP loads the image from the MX.

The forced image download option is not applicable to MP models MP-52, MP-101, and MP-122.

Examples The following command enables forced image download on Distributed MP 69:

```
MX# set ap 69 force-image-download enable
success: change accepted.
```

See Also **show ap config radio** on page 12-320

set ap group

Deprecated in MSS Version 6.0. To configure RF load balancing, see **set load-balancing mode** on page 12-255.

set ap image

Loads an AirDefense sensor software image on an MP.

Syntax **set ap** *apnum* **image** *filename*

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
filename	Name of the AirDefense sensor software image file. This file is assumed to have been copied to the MX.

Defaults None.

Access Enabled.

History

Version 5.0	Command introduced.
Version 6.0	Option **dap** removed.
Version 6.2	Added the index value range of 1 to 9999.

Usage After the AirDefense sensor software is copied to the MX, use this command to configure an MP to load the software. When you do this, the software is transferred to the MP, which then reboots and comes up as an AirDefense sensor.

Examples The following command causes Distributed MP 1 to load the file, then reboot as an AirDefense sensor:

```
MX# set ap 1 image adconvert.bin
This will change the file a AP will boot. Would you like to continue? (y/n) [n] y
```

See Also **clear ap image** on page 12-222

set ap local-switching mode

Enables local switching for a specified MP.

Syntax **set ap** *apnum* **local-switching mode** {**enable** | **disable**}

apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
enable	Enables local switching for the MP.
disable	Disables local switching for the MP.

Defaults Local switching is disabled by default.

Access Enabled.

History

Version 6.0	Command introduced.
Version 6.2	Added the index value range of 1 to 9999.

Usage Local switching allows traffic for specified VLANs to be switched by the MP, instead of tunneling traffic back to an MX. The VLANs that perform local switching are specified in a VLAN profile.

Local switching can be enabled on MPs connected to the MX through an intermediate Layer 2 or Layer 3 network. Local switching is not supported for MPs that are directly connected to an MX.

If local switching is enabled on an MP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named that is not tagged.

Examples The following command enables local switching for MP 7:

```
MX# set ap 7 local-switching mode enable
success: change accepted.
```

See Also

- **set ap local-switching vlan-profile** on page 12-242
- **set vlan-profile** on page 6-75

set ap local-switching vlan-profile

Applies a specified VLAN profile to an MP to use with local switching.

Syntax **set ap** *apnum* **local-switching vlan-profile** *profile-name*

apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
profile-name	The name of a VLAN profile configured on the MX.

Defaults If local switching is enabled on an MP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named that is not tagged.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to an MP, traffic for the VLANs specified in the VLAN profile is locally switched by the MP instead of tunneling the traffic back to an MX.

When applying a VLAN profile causes traffic that was tunneled to an MX to be locally switched by MPs, or vice-versa, the sessions of clients associated with the MPs with the applied VLAN profile are terminated, and the clients must re-associate with the MPs.

Examples The following command specifies that MP 7 use VLAN profile :

```
MX# set ap 7 local-switching vlan-profile locals
success: change accepted.
```

See Also

- **set ap local-switching mode** on page 12-242
- **clear ap local-switching vlan-profile** on page 12-223
- **set vlan-profile** on page 6-75

set ap name

Changes an MP name.

Syntax **set ap** *apnum* **name** *name*

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
name	Alphanumeric string of up to 16 characters, with no spaces.

Defaults The default name of a directly attached MP is based on the port number of the MP access port attached to the MP. For example, the default name for an MP on MP access port 1 is .

Access Enabled.

History

Version 1.0	Command introduced
Version 2.0	Option **dap** added for Distributed MPs
Version 4.1	Default Distributed MP name changed from DMP to DAP
Version 6.0	Option **dap** removed.
Version 6.2	Added index value range from 1 to 9999.

Examples The following command changes the name of the MP on port 1 to :

```
MX# set ap 1 name techpubs
success: change accepted.
```

See Also **show ap config radio** on page 12-320

set ap radio antenna-location

Specifies the location (indoors or outdoors) of an external antenna. Use this command to ensure that the proper set of channels is available on the radio. In some cases, the set of valid channels for a radio differs depending on whether the antenna is located indoors or outdoors.

Syntax **set ap** *apnum* **radio** *number* **antenna-location** {**indoors** | **outdoors**}

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
radio *number*	Specify radio 1 or radio 2.
antenna-location	Specify antenna location.
indoors	Specifies that the external antenna is installed indoors (inside the building).
outdoors	Specifies that the external antenna is installed outdoors.

Defaults The default antenna location is **indoors**.

Access Enabled.

History Introduced in MSS 5.0.

Examples The following command sets the antenna location for radio 1 on Distributed MP 22 to **outdoors**:

```
MX# set ap 22 radio 1 antenna-location outdoors
success: change accepted.
```

See Also **set ap radio antennatype** on page 12-244

set ap radio antennatype

Sets the model number for an external antenna.

set ap *apnum* **radio** {**1** | **2**} **antennatype {ANT1060 | ANT1120 | ANT1180 | ANT5060 | ANT5120 | ANT5180 | ANT-1360-OUT | ANT-5360-OUT | ANT-5060-OUT | ANT-5120-OUT | internal}**

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
radio 1	Radio 1 of the MP.
radio 2	Radio 2 of the MP. (This option does not apply to single-radio models.)
antennatype {**ANT1060 | ANT1120 | ANT1180 | internal**}	MP-3 and MP-262 802.11b/g external antenna models: ❑ ANT1060—60° 802.11b/g antenna ❑ ANT1120—120° 802.11b/g antenna ❑ ANT1180—180° 802.11b/g antenna ❑ internal—Uses the internal antenna instead
antennatype {**ANT5060 | ANT5120 | ANT5180 | internal**}	MP-3 802.11a external antenna models: ❑ ANT5060—60° 802.11a antenna ❑ ANT5120—120° 802.11a antenna ❑ ANT5180—180° 802.11a antenna ❑ internal—Uses the internal antenna instead

antennatype {ANT-1360-OUT | ANT-5360-OUT | ANT-5060-OUT | ANT-5120-OUT | internal}	MP-620 external antenna models: ❑ ANT-1360-OUT—360° 802.11b/g antenna ❑ ANT-5360-OUT—360° 802.11a antenna ❑ ANT-5060-OUT—60° 802.11a antenna ❑ ANT-5120-OUT—120° 802.11a antenna ❑ internal—Uses the internal antenna instead

Defaults All radios use the internal antenna by default, if the MP model has an internal antenna. The MP-620 802.11b/g radio uses model ANT-1360-OUT by default. The MP-620 802.11a radio uses model ANT-5360-OUT by default. The MP-262 802.11b/g radio uses model ANT1060 by default.

Access Enabled.

History

Version 2.1	Command introduced
Version 3.2	❑ Model numbers added for 802.11a external antennas. ❑ Default changed to internal (except for the MP-262).
Version 4.1	Model numbers added for MP-620 external antennas.
Version 6.2	Added index value range of 1 to 9999.

Usage This command applies only to radios on MP models MP-3 and MP-620 and to the 802.11b/g radio on model MP-262.

Examples The following command configures the 802.11b/g radio on Distributed MP 1 to use antenna model ANT1060:

```
MX# set ap 1 radio 1 antennatype ANT1060
success: change accepted.
```

See Also **show ap config radio** on page 12-320

set ap radio auto-tune max-power

Sets the maximum power that RF Auto-Tuning can set on a radio.

Syntax **set ap** {*apnum* | **auto**} **radio** {**1** | **2**} **auto-tune max-power** *power-level*

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
ap auto	Sets the maximum power for radios configured by the MP configuration profile. (See **set ap auto** on page 12-229.)
radio 1	Radio 1 of the MP.
radio 2	Radio 2 of the MP. (This option does not apply to single-radio models.)
power-level	Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation. The can be a value from 1 to 20.

Defaults The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access Enabled.

History

Examples

See Also

- **set ap boot-configuration mesh ssid** on page 12-237
- **set service-profile mesh** on page 12-293
- **show ap mesh-links** on page 12-330

set ap radio load-balancing

Disables or enables RF load balancing for an MP radio.

Syntax **set ap** *apnum* **radio** {**1** | **2**} **load-balancing** {**enable** | **disable**}

Defaults RF load balancing is enabled by default for all MP radios.

Access Enabled.

History

Usage By default, RF load balancing is enabled on all MP radios. Use this command to disable or re-enable RF load balancing for the specified MP radio.

RF load balancing can also be disabled or re-enabled globally with the **set load-balancing mode** command. If RF load balancing has been enabled or disabled for a specific MP radio, then the

Syntax **set ap** *apnum* **radio** {**1** | **2**} **load-balancing group** *name* [**rebalance**]

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
radio 1	Radio 1 of the MP.
radio 2	Radio 2 of the MP. (This option does not apply to single-radio models.)
group *name*	Name of an RF load balancing group to which the MP radio is assigned. A radio can belong to only one group.
rebalance	Configures the MP radio to disassociate client sessions and rebalance them whenever a new MP radio is added to the load balancing group.

Defaults By default, MP radios are not part of an RF load balancing group.

Access Enabled.

History

Version 6.0	Command introduced.
Version 6.2	Added index valued range from 1 to 9999.

Usage Assigning radios to specific load balancing groups is optional. When you do this, MSS considers them to have exactly overlapping coverage areas, rather than using signal strength calculations to determine their overlapping coverage. MSS attempts to distribute client sessions across radios in the load balancing group evenly. A radio can be assigned to only one group.

Examples The following command assigns MP radio 1 on MP 7 to load balancing group :

```
MX# set ap 7 radio 1 load-balancing group room1
MX#
```

See Also

- **set load-balancing strictness** on page 12-255
- **clear ap radio load-balancing group** on page 12-226
- **set ap local-switching mode** on page 12-242
- **show load-balancing group** on page 12-343

set ap radio mode

Enables or disables a radio on an MP.

Syntax **set ap** {*apnum* | **auto**}} **radio** {**1** | **2**} **mode** {**enable** |**sentry**| **disable**}

ap *apnum*	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
ap auto	Sets the radio mode for MPs managed by the MP configuration profile. (See **set ap auto** on page 12-229.)
radio 1	Radio 1 of the MP.
radio 2	Radio 2 of the MP. (This option does not apply to single-radio models.)
mode enable	Enables a radio.
mode sentry	Allows longer dwell times on scanning channels.
mode disable	Disables a radio.

Defaults MP access point radios are disabled by default.

Access Enabled.

History

Usage To enable or disable one or more radios assigned to a profile, use the **set ap radio radio-profile** command. To enable or disable all radios that use a specific radio profile, use the **set radio-profile** command.

Examples The following command enables radio 1 on MP 1:

```
MX# set ap 1 radio 1 mode enable
success: change accepted.
```

The following command sets radio 2 in sentry mode on MP 1:

```
MX# set ap 1 radio 2 mode sentry
success: change accepted.
```

See Also

- **clear ap radio** on page 12-224
- **set ap radio radio-profile** on page 12-251
- **set radio-profile mode** on page 12-269
- **show ap config radio** on page 12-320

Defaults The default transmit power on all MP radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access Enabled.

History

Usage You also can configure a radio channel on the same command line. Use the **channel**

Syntax **set ap security** *secsetting* {**require** | **optional** | **none**}

set load-balancing mode

Disables or enables RF load balancing globally on the MX.

Syntax **set load-balancing mode** {**enable** | **disable**}

Defaults RF load balancing is enabled by default.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage By default, RF load balancing is enabled on all MP radios. Use this command to disable or re-enable RF load balancing globally for all MP radios managed by the MX.

If RF load balancing has been enabled or disabled for a specific MP radio, r0 -952 ban.360.8(rab)-4.3e thvthdu

Use this command to specify how strictly MSS attempts to keep the client load balanced across the MP radios in the load-balancing group. When strictness is specified (the default), MSS

Even when RF Auto-Tuning for channels is enabled, MSS does not change the channel on radios that have active client sessions, unless you use the **ignore-clients** option.

Examples The following command disables dynamic channel tuning for radios in the radio profile:

```
#X# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

See Also

- **set ap radio channel** on page 12-246
- **set radio-profile auto-tune channel-holddown** on page 12-258
- **set radio-profile auto-tune channel-interval** on page 12-258
- **set radio-profile auto-tune power-config** on page 12-260
- **show radio-profile** on page 12-344

set radio-profile auto-tune channel-holddown

Sets the minimum number of seconds a radio in a radio profile must remain on the current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

Syntax **set radio-profile** *profile-name* **auto-tune channel-holddown** *holddown*

profile-name	Radio profile name.
rate	#inimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

Defaults The default RF Auto-Tuning channel holddown is 900 seconds.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.

Examples The following command changes the channel holddown for radios in radio profile to 600 seconds:

```
#X# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

See Also

- **set radio-profile auto-tune 11a-channel-range** on page 12-256
- **set radio-profile auto-tune channel-interval** on page 12-258
- **set radio-profile auto-tune channel-lockdown** on page 12-259
- **show radio-profile** on page 12-344

set radio-profile auto-tune channel-interval

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

Syntax **set radio-profile** *profile-name* **auto-tune channel-interval** *seconds*

profile-name	Radio profile name.
seconds	Number of seconds RF Auto-Tuning waits before changing radio channels to

Defaults The default channel interval is 3600 seconds (one hour).

Access Enabled.

History Introduced in MSS Version 3.0.

Usage It is recommended to use an interval of at least 300 seconds (5 minutes).

RF Auto-Tuning can change a radio channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.

Examples The following command sets the channel interval for radios in radio profile to 2700 seconds (45 minutes):

```
MX# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

See Also

- **set radio-profile auto-tune 11a-channel-range** on page 12-256
- **set radio-profile auto-tune channel-holddown** on page 12-258
- **set radio-profile auto-tune channel-lockdown** on page 12-259
- **show radio-profile** on page 12-344

set radio-profile auto-tune channel-lockdown

Locks down the current channel settings on all radios in a radio profile. The channel settings that are in effect when the command is entered are changed into statically configured channel assignments on the radios. RF Auto-Tuning of channels is then disabled in the radio profile.

Syntax **set radio-profile** *profile-name* **auto-tune channel-lockdown**

Defaults By default, when RF Auto-Tuning of channels is enabled, channels continue to be changed dynamically based on network conditions.

Access Enabled.

History Introduced in MSS Version 5.0.

Usage To save this command and the static channel configuration commands created when you enter this command, save the configuration.

Examples The following command locks down the channel settings for radios in radio profile :

```
MX# set radio-profile rp2 auto-tune channel-lockdown
success: change accepted.
```

See Also

- **set radio-profile auto-tune 11a-channel-range** on page 12-256
- **set radio-profile auto-tune channel-holddown** on page 12-258

- **set radio-profile auto-tune channel-interval** on page 12-258
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **show radio-profile** on page 12-344

set radio-profile auto-tune power-backoff-timer

Deprecated in MSS Version 5.0.

set radio-profile auto-tune ignore-clients

Ignores client connections in auto-tune channel selections.

Syntax **set radio-profile** *profile-name* **auto-tune ignore-clients {enable | disable}**

profile-name	Radio profile name.
enable	Configures auto-tune to ignore client connections.
disable	Disables the feature.

Defaults None

Access Enabled

History Introduced in MSS 6.0.

set radio-profile auto-tune power-config

Enables or disables dynamic power tuning (RF Auto-Tuning) for the MP radios in a radio profile.

Syntax **set radio-profile** *name* **auto-tune power-config** {**enable** | **disable**}

name	Radio profile name.
enable	Configures radios to dynamically set power levels when the MPs are started.
disable	Configures radios to use statically assigned power levels, or the default power levels if unassigned, when the radios are started.

Defaults Dynamic power assignment is disabled by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage When RF Auto-Tuning for power is disabled, MSS does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, MSS does not allow you to manually change the power level.

Examples The following command enables dynamic power tuning for radios in the radio profile:

```
MX# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 12-245

- **set radio-profile auto-tune 11a-channel-range** on page 12-256
- **set radio-profile auto-tune power-interval** on page 12-261
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **show radio-profile** on page 12-344

set radio-profile auto-tune power-interval

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

Syntax **set radio-profile** *name* **auto-tune power-interval** *seconds*

name	Radio profile name.	Radio profile name.	Radio profile name.

Defaults The default power tuning interval is 600 seconds.

Access Enabled.

History Introduced in MSS Version 3.0.

Examples The following command sets the power interval for radios in radio profile to 240 seconds:

```
MX# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 12-245
- **set radio-profile auto-tune power-config** on page 12-260
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **set radio-profile auto-tune power-ramp-interval** on page 12-262
- **show service-profile** on page 12-347

set radio-profile auto-tune power-lockdown

Locks down the current power settings on all radios in a radio profile. The power settings that are in effect when the command is entered are changed into statically configured power settings on the radios. RF Auto-Tuning of power is then disabled in the radio profile.

Syntax **set radio-profile** *name* **auto-tune power-lockdown**

Defaults By default, when RF Auto-Tuning of power is enabled, power settings continue change dynamically based on network conditions.

Access Enabled.

History Introduced in MSS Version 5.0.

Usage To save this command and the static power configuration commands created when you enter this command, save the configuration.

Examples The following command locks down the power settings for radios in radio profile :

```
MX# set radio-profile rp2 auto-tune power-lockdown
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 12-245
- **set radio-profile auto-tune channel-lockdown** on page 12-259
- **set radio-profile auto-tune power-config** on page 12-260
- **set radio-profile auto-tune power-interval** on page 12-261
- **set radio-profile auto-tune power-ramp-interval** on page 12-262
- **show radio-profile** on page 12-344

set radio-profile auto-tune power-ramp-interval

Changes the interval at which power is increased or decreased, in 1 dBm increments, on radios in a radio profile until the optimum power level calculated by RF Auto-Tuning is reached.

Syntax **set radio-profile** *profile-name* **auto-tune power-ramp-interval** *seconds*

profile-name	Radio profile name.
seconds	Number of seconds MSS waits before increasing or decreasing radio power by another 1 dBm. You can specify from 1 to 65535.

Defaults The default interval is 60 seconds.

Access Enabled.

History Introduced in MSS Version 5.0.

Examples The following command changes the power ramp interval for radios in radio profile to 120 seconds:

```
MX# set radio-profile rp2 auto-tune power-ramp-interval 120
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 12-245
- **set radio-profile auto-tune power-config** on page 12-260
- **set radio-profile auto-tune power-interval** on page 12-261
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **show radio-profile** on page 12-344

set radio-profile beacon-interval

Changes the rate at which each MP radio in a radio profile advertises its service set identifier (SSID).

Syntax **set radio-profile** *profile-name* **beacon-interval** *interval*

profile-name	Radio profile name.
interval	Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms.

Defaults The beacon interval for MP radios is 100 ms by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command changes the beacon interval for radio profile to 200 ms:

```
MX# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

See Also

- **set radio-profile mode** on page 12-269
- **show radio-profile** on page 12-344

set radio-profile cac background

Sets Quality of Service (QoS) options for a radio profile.

Syntax **set radio-profile** *profile-name* **cac background {max-utilization** *percentage* **| mode [enable | disable] | policing [enable | disable]}**

profile-name	Name of radio profile.
max-utilization *percentage*	Set maximum admission control limit for background traffic. You can configure a percentage from 1 to 100 percent.
mode	Configures CAC to be mandatory for the radio profile.
policing	Configure admission control policing for the radio profile.

Defaults None

Access Enabled

History Introduced in MSS Version 7.0.

set radio-profile cac best-effort

Sets Quality of Service (QoS) options for a radio profile.

Syntax **set radio-profile** *profile-name* **cac best-effort {max-utilization** *percentage* **| mode [enable | disable] | policing [enable | disable]}**

profile-name	Name of radio profile.
max-utilization *percentage*	Set maximum admission control limit for best effort traffic. You can configure a percentage from 1 to 100 percent.
mode	Configures CAC to be mandatory for the radio profile.
policing	Configure admission control policing for the radio profile.

Defaults None

Access Enabled

Introduced in MSS Version 7.0.

set radio-profile cac video

Syntax **set radio-profile** *profile-name* **cac video {max-utilization** *percentage* **| mode [enable | disable] | policing [enable | disable]}**

profile-name	Name of radio profile.
max-utilization *percentage*	Set maximum admission control limit for video traffic. You can configure a percentage from 1 to 100 percent.
mode	Configures CAC to be mandatory for the radio profile.
policing	Configure admission control policing for the radio profile.

Defaults None

Access Enabled

History Introduced in MSS Version 7.0.

set radio-profile cac voice

Sets Quality of Service (QoS) options for a radio profile.

Syntax **set radio-profile** *profile-name* **cac voice {max-utilization** *percentage* **| mode [enable | disable] | policing [enable | disable]}**

profile-name	Name of radio profile.
max-utilization *percentage*	Set maximum admission control limit for voice traffic. You can configure a percentage from 1 to 100 percent.
mode	Configures CAC to be mandatory for the radio profile.
policing	Configure admission control policing for the radio profile.

Defaults None

Access Enabled

History Introduced in MSS Version 7.0.

set radio-profile countermeasures

Enables or disables countermeasures on the MP radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.

MP radios can also issue countermeasures against interfering devices. An interfering device is not part of the Trapeze network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any MX in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with MP radios.

Syntax **set radio-profile** *profile-name* **countermeasures** {**all** | **rogue** | **none**}

profile-name	Radio profile name.
all	Configures radios to attack rogues and interfering devices.
rogue	Configures radios to attack rogues only.
none	Disables countermeasures for this radio profile.

Defaults Countermeasures are disabled by default.

Access Enabled.

History

Version 4.0	Command introduced.
Version 4.1	New option **configured** added to support on-demand countermeasures.
Version 7.0	The option **configured** was removed.

Examples The following command enables countermeasures in radio profile for rogues only:

```
MX# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile :

```
MX# clear radio-profile radprof3 countermeasures
success: change accepted.
```

The following command causes radios managed by radio profile to issue countermeasures against devices in the MX switch's attack list:

```
MX# set radio-profile radprof3 countermeasures configured
success: change accepted.
```

Note that when you issue this command, countermeasures are then issued only against devices in the MX attack list, not against other devices that were classified as rogues by other means.

set radio-profile dfs-channels

Enables the use of DFS channels to meet regulatory requirements.

Syntax **set radio-profile** *profile-name* **dfs channels {enable | disable}**

Defaults None

Access Enabled

History Introduced in MSS 7.0.

set radio-profile dtim-interval

Changes the number of times after every beacon that each MP radio in a radio profile sends a delivery traffic indication map (DTIM). An MP sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.

Syntax **set radio-profile** *profile-name* **dtim-interval** *interval*

Defaults By default, MPs send the DTIM once after each beacon.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You must disable all radios using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The DTIM interval does not apply to unicast frames.

Examples The following command changes the DTIM interval for radio profile to 2:

```
MX# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

See Also

- **set radio-profile mode** on page 12-269
- **show radio-profile** on page 12-344

set radio-profile weighted-fair-queuing

Configures a minimum service level to specific radio profiles. Medium time weights determine the relative transmit utilization of the radio between service profiles.

Syntax **set radio-profile** *profile-name* **weighted-fair-queuing** {**enable** | **disable**} **weight** *service-profile-name weight*

weighted-fair-queuing disable	Disable weighted queuing.
service-profile-name	Name of the service profile to apply weighted queuing.
weight	Configure a weight value from 1 to 100. All profiles with

Defaults None

Access Enabled

History Introduced in MSS Version 6.2.

Examples To configure weighted queuing for a service and radio profile, use the following command:

```
MX# set radio-profile wireless weighted-fair-queuing enable weight mp_conference 25
success: change accepted.
```

set radio-profile frag-threshold

Changes the fragmentation threshold for the MP radios in a radio profile. The fragmentation threshold is the threshold at which the long-retry-count is applicable instead of the short-retry-count.

The long-retry-count specifies the number of times a radio can send a unicast frame that is equal to or longer than the frag-threshold without receiving an acknowledgment.

The short-retry-count specifies the number of times a radio can send a unicast frame that is shorter than the frag-threshold without receiving an acknowledgment.

Syntax **set radio-profile** *name* **frag-threshold** *threshold*

Defaults The default fragmentation threshold for MP radios is 2346 bytes.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The frag-threshold does not specify the maximum length a frame is allowed to be without being broken into multiple frames before transmission. The MP does not support fragmentation upon transmission, only upon reception.

The frag-threshold does not change the RTS threshold, which specifies the maximum length of a frame before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use the **set radio-profile rts-threshold** command instead.

Examples The following command changes the fragmentation threshold for radio profile to 1500 bytes:

```
MX# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

See Also

- **set radio-profile mode** on page 12-269
- **set radio-profile rts-threshold** on page 12-275

- **set service-profile long-retry-count** on page 12-292
- **set service-profile short-retry-count** on page 12-298
- **show radio-profile** on page 12-344

set radio-profile long-retry

Deprecated in MSS Version 4.2. In 4.2, this parameter is associated with service profiles instead of radio profiles. See **set service-profile long-retry-count** on page 12-292.

set radio-profile max-rx-lifetime

Changes the maximum receive threshold for the MP radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame by a radio can remain in buffer memory.

Syntax **set radio-profile** *name* **max-rx-lifetime** *time*

Defaults The default maximum receive threshold for MP radios is 2000 ms (2 seconds).

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command changes the maximum receive threshold for radio profile to 4000 ms:

```
MX# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

See Also

- **set radio-profile mode** on page 12-269
- **set radio-profile max-tx-lifetime** on page 12-268
- **show radio-profile** on page 12-344

set radio-profile max-tx-lifetime

Changes the maximum transmit threshold for the MP radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that -.0028 623(emi0d.c1/TT24 1 Tf403.32 TTD.0012sche

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile**

preamble-length	**short**	Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client. **Note:** This parameter applies only to 802.11b/g radios.
qos-mode	**wmm**	Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of MP radios for Wi-Fi Multimedia (WMM).
rfid-mode	**disable**	Radio does not function as a location receiver in an AeroScout Visibility System.
rts-threshold	**2346**	Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method.
service-profile	No service profiles defined	You must configure a service profile. The service profile sets the SSID name and other parameters.
wmm-powersave	**disable**	Requires clients to send a separate PSpoll to retrieve each unicast packet buffered by the MP radio.

Access Enabled.

History

Version 1.0 Command introduced

Version 3.0
- Parameters that no longer apply to radio profiles in MSS Version 3.0 removed:
  - **auth-dot1x**
  - **auth-psk**
  - **beaconed-ssid**
  - **cipher-ccmp**
  - **cipher-tkip**
  - **cipher-wep104**
  - **cipher-wep40**
  - **clear-ssid**
  - **crypto-ssid**
  - **psk-phrase**
  - **psk-raw**
  - **shared-key-auth**
  - **tkip-mc-time**
  - **wep key-index**
  - **wep active-multicast-index**
  - **wep active-unicast-index**
  - **wpa-ie**
- **auto-tune** and **service-profile**

Usage Use the command without any optional parameters to create new profile. If the radio profile does not already exist, MSS creates a new radio profile. Use the **enable** or **disable** option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the **set ap radio** command.

Examples The following command configures a new radio profile named :

```
MX# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile :

```
MX# set radio-profile rp1 mode enable
```

The following commands disable the radios that use radio profile , change the beacon interval, then reenable the radios:

```
MX# set radio-profile rp1 mode disable
MX# set radio-profile rp1 beacon-interval 200
MX# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on MP radios in radio profile :

```
MX# set radio-profile rp2 wpa-ie enable
success: change accepted.
```

See Also

- **set ap radio mode** on page 12-249
- **set ap radio radio-profile** on page 12-251
- **show ap config radio** on page 12-320
- **show radio-profile** on page 12-344

set radio-profile preamble-length

Changes the preamble length for which an 802.11b/g MP radio advertises support. This command does not apply to 802.11a.

Syntax **set radio-profile** *name* **preamble-length** {**long** | **short**}

name	Radio profile name.
long	Advertises support for long preambles.
short	Advertises support for short preambles.

Defaults The default is **short**.

Access Enabled.

History

Version 1.0	Command introduced.
Version 1.1	Default changed from **long** to **short**.

Usage Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (**short** or **long**), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

Syntax **set radio-profile** *name* **rate-enforcement** {**enable** | **disable**}

Defaults Data rate enforcement is disabled by default.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage Each type of radio (802.11a, 802.11b, and 802.11g) providing service to an SSID has a set of radio rates allowed for use when sending beacons, multicast frames, and unicast data. You can configure the rate set for each type of radio, specifying rates in three categories:

- Mandatory – Valid 802.11 transmit rates that clients must support in order to associate with the MP
- Disabled – Valid 802.11 transmit rates are disabled. MPs do not transmit at the disabled rates
- Standard – Valid 802.11 transmit rates that are not disabled and are not mandatory

By default, the rate set is not enforced, meaning that a client can associate with and transmit data to the MP using a disabled data rate, although the MP does not transmit data back to the client at the disabled rate.

You can use this command to enforce the data rates, which means that a connecting client transmit at one of the mandatory or standa 4 TD.1(t)2i-6.1(–)5..2.3(asnse thise to eei)4.bl.00575 associat6(wit

See Also

- **set radio-profile mode**

attr	No attributes configured	Does not assign the SSID authorization attribute values to SSID users, even if attrib8 M( )6.7ware(noto thrwise( )]TJ-11.2067 -1 TD(ients.e

web-portal-acl	**portalacl** **Note:** This is the default only if the fallthru type on the service profile has been set to **web-portal**. Otherwise, the value is unconfigured.	If set to **portalacl** and the service profile fallthru is set to **web-portal**, radios use the ACL to filter traffic for Web Portal users during authentication. If the fallthru type is **web-portal** but **web-portal-acl** is set to an ACL other than , the other ACL is used. If the fallthru type is not **web-portal**, radios do not use the **web-portal-acl** setting.
web-portal-form	Not configured	For WebAAA users, serves the Trapeze Networks login page.
web-portal-logout	**none**	If set to logout-url, you can define a custom URL that allows a client to log out of the network. To enable this feature, use the **mode** option and then **enable**.
web-portal-session-timeout	**5**	Allows a Web Portal WebAAA session to remain in the Deassociated state 5 seconds before being terminated automatically.
wep key-index	No keys defined	Uses dynamic WEP rather than static WEP. **Note:** If you configure a WEP key for static WEP, MSS continues to also support dynamic WEP.
wep active-multicast-index	**1**	Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined.
wep active-unicast-index	**1**	Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined.
wpa-ie	**disable**	Does not use the WPA IE in transmitted frames.

Access Enabled.

History Introduced in MSS Version 3.0.

Version 3.0	Command introduced.
Version 7.0	The option **static-cos** was removed.

Usage You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command maps service-profile to radio profile :

```
MX# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

See Also

- **set service-profile attr** on page 12-281
- **set service-profile auth-dot1x** on page 12-282
- **set service-profile auth-fallthru** on page 12-283
- **set service-profile auth-psk** on page 12-284
- **set service-profile beacon** on page 12-284
- **set service-profile cac-mode** on page 12-286
- **set service-profile cac-session** on page 12-286

Syntax set service-profile p*rofile-name* 11n a-mpdu-max-length [8K | 16K | 32K | 64K] a-msdu-max-length [4K | 8K] frame-aggregation [msdu | mpdu | all | disable] short-guard-interval [enable | disable]

profile-name	Name of the service profile.
a-mpdu-max-length	Configures the length of the MPDU packet in kilobytes. Select from 8, 16, 32, or 64K.
a-msdu-max-length	Configures the length of the MSDU packet in kilobytes. Select from 8, 16, 32, or 64K.
frame-aggregation	Enables aggregation of MPDU and MSDU packets. Select either MPDU or MSDU or all. You can also disable this option.
short-guard-interval	Configure this option to prevent inter-symbol interference on the 802.11n network.

Defaults None

Access Enabled

History Introduced in MSS Version 7.0.

Usage

set service-profile attr

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

Syntax **set service-profile** *profile-name* **attr** *attribute-name value*

profile-name	Service profile name.
attribute-name value	Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 9– 9 on page 178. All of the attributes listed in **Table 9– 9** can be used with this command except **ssid**.

Defaults By default, a service profile does not have any authorization attributes set.

Access Enabled.

History Introduced in MSS 4.1.

Usage To change the value of a default attribute for a service profile, use the **set service-profile attr** command and specify a new value.

The SSID default attributes are applied to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the **service-type** attribute set to . If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the

vlan-name attribute set to , then that user has a total of two attributes set: **service-type** and

Examples The following command disables 802.1X authentication for WPA clients that use service profile :

```
MX# set service-profile wpa_clients auth-dot1x disable
success: change accepted.
```

See Also

- **set service-profile auth-psk** on page 12-284
- **set service-profile psk-phrase** on page 12-295
- **set service-profile wpa-ie** on page 12-314
- **show service-profile** on page 12-347

set service-profile auth-fallthru

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, MSS checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authenticatio13 Tc1.7(di)-bl6 0 match a

Syntax **set service-profile** *name* **beacon** {**enable** | **disable**}

Defaults Beaconing is enabled by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Examples The following command disables beaconing of the SSID managed by service profile :

```
MX# set service-profile sp2 beacon disable
success: change accepted.
```

See Also

- **set radio-profile beacon-interval** on page 12-263
- **set service-profile ssid-name** on page 12-303
- **set service-profile ssid-type** on page 12-304
- **show service-profile** on page 12-347

set service-profile bridging

Enables wireless bridging for a service profile configured for WLAN mesh services.

Syntax **set service-profile** *service-profile* **bridging** {**enable** | **disable**}

Defaults None.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage WLAN mesh services can be used in a wireless bridge configuration, implementing MPs as

See Also

- **set ap boot-configuration mesh ssid** on page 12-237
- **set service-profile mesh** on page 12-293
- **show ap mesh-links** on page 12-330

See Also

- **set service-profile cac-mode** on page 12-286
- **show service-profile** on page 12-347

set service-profile cipher-ccmp

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

Syntax **set service-profile** *name* **cipher-ccmp** {**enable** | **disable**}

name	Service profile name.
enable	Enables CCMP encryption for WPA clients.
disable	Disables CCMP encryption for WPA clients.

Defaults CCMP encryption is disabled by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage To use CCMP, you must also enable the WPA IE.

Examples The following command configures service profile to use CCMP encryption:

```
MX# set service-profile sp2 cipher-ccmp enable
success: change accepted.
```

See Also

- **set service-profile cipher-tkip** on page 12-287
- **set service-profile cipher-wep104** on page 12-288
- **set service-profile cipher-wep40** on page 12-289
- **set service-profile wpa-ie** on page 12-314
- **show service-profile** on page 12-347

set service-profile cipher-tkip

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

Syntax **set service-profile** *name* **cipher-tkip** {**enable** | **disable**}

name	Service profile name.
enable	Enables TKIP encryption for WPA clients.
disable	Disables TKIP encryption for WPA clients.

Defaults When the WPA IE is enabled, TKIP encryption is enabled by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage To use TKIP, you must also enable the WPA IE.

Examples The following command disables TKIP encryption in service profile :

```
MX# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

See Also

-

set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

Syntax **set service-profile** *name* **cipher-wep40** {**enable** | **disable**}

name	Service profile name.
enable	Enables 40-bit WEP encryption for WPA clients.
disable	Disables 40-bit WEP encryption for WPA clients.

Defaults 40-bit WEP encryption is disabled by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Examples The following command configures service profile to use 40-bit WEP encryption:

```
MX# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

See Also

- **set service-profile cipher-ccmp** on page 12-287
- **set service-profile cipher-tkip** on page 12-287
- **set service-profile cipher-wep104** on page 12-288
- **set service-profile wep key-index** on page 12-313
- **set service-profile wpa-ie** on page 12-314
- **show service-profile** on page 12-347

set service-profile cos

Sets the Class-of-Service (CoS) level for static CoS.

Syntax **set service-profile** *profile-name* **cos** *level*

profile-name	Service profile name.
level	CoS value assigned by the MP to all traffic in the service profile.

Defaults The default static CoS level is 0.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage This command applies only when static CoS is enabled. If static CoS is disabled, prioritization is based on the QoS mode configured in the radio profile, and on any ACLs that set CoS. (See the “Configuring Quality of Service” chapter of the .) To enable static CoS, use the **set service-profile static-cos** command.

Examples The following command changes the static CoS level to 7 (voice priority):

```
MX# set service-profile sp1 cos 7
success: change accepted.
```

See Also

- **set service-profile static-cos** on page 12-304
- **show service-profile** on page 12-347

set service-profile dhcp-restrict

Enables or disables DHCP Restrict on a service profile. DHCP Restrict filters the traffic from a newly associated client and allows DHCP traffic only, until the client has been authenticated and authorized. All other traffic is captured by the MX and is not forwarded. After the client is successfully authorized, the traffic restriction is removed.

Syntax **set service-profile** *profile-name* **dhcp-restrict** {**enable** | **disable**}

Defaults DHCP Restrict is disabled by default.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage

Syntax **set service-profile** *profile-name* **idle-client-probing** {**enable** | **disable**}

Defaults Idle-client probing is enabled by default.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the **user-idle-timeout** command.

Examples The following command disables idle-client keepalives on service profile :

```
MX# set service-profile sp1 idle-client-probing disable
success: change accepted.
```

See Also

- **set service-profile user-idle-timeout** on page 12-308
- **show service-profile** on page 12-347

set service-profile keep-initial-vlan

Configures MP radios managed by the radio profile to leave a roamed user on the VLAN assigned by the MX where the user logged on. When this option is disabled, a users VLAN is reassigned by each MX when a user roams.

Syntax **set service-profile** *profile-name* **keep-initial-vlan** {**enable** | **disable**}

Defaults This option is disabled by default.

Access Enabled.

See Also **show service-profile** on page 12-347

set service-profile load-balancing-exempt

Exempts a service profile from performing RF load balancing.

Syntax **set service-profile** *profile-name* **load-balancing-exempt** {**enable** | **disable**}

profile-name	Service profile name.
enable	Exempts the specified service profile from RF load balancing.
disable	If a service profile has previously10.8 105.3 7ly10.8 105. ex0.8 10m/TT bal.8 10m(o)-2D.0006373Tc.0047

Defaults By default, MP radios automatically perform RF load balancing for all service profiles.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage Use this command to exempt a service profile from RF load balancing. Exempting a service profile from RF load balancing means that if an MP radio is attempting to steer clients away, the radio does not reduce or conceal the availability of the SSID named in the exempted service profile. Even if a radio is withholding probe responses to manage the load, the radio does respond to probes for an exempt SSID. Also, if an MP radio is withholding probe responses, and a client probes for SSID, and the radio has at least one exempt SSID, the radio responds to the probe, but the response reveals only the exempt SSID(s).

Examples The following command exempts service profile from RF load balancing:

```
MX# set service-profile sp3 load-balancing-exempt enable
success: change accepted.
```

See Also

- **set load-balancing strictness** on page 12-255
- **set ap radio load-balancing** on page 12-248
- **set ap local-switching mode** on page 12-242
- **show load-balancing group** on page 12-343

set service-profile long-retry-count

Changes the long retry threshold for a service profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the frag-threshold.

Syntax **set service-profile** *name* **long-retry-count** *threshold*

Defaults The default long unicast retry threshold is 5 attempts.

Access Enabled.

History Introduced in MSS Version 4.2.

See Also

- **set ap boot-configuration mesh ssid** on page 12-237
- **show ap mesh-links** on page 12-330

set service-profile no-broadcast

Disables or reenables the no-broadcast mode. The no-broadcast mode helps reduce traffic overhead on an SSID by having more SSID bandwidth available for unicast traffic. The no-broadcast mode also helps VoIP

Syntax **set service-profile** *profile-name* **psk-phrase** *passphrase*

profile-name	Service profile name.
passphrase	An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

Defaults None.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the MX configuration. Neither the binary number nor the passphrase is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples The following command configures service profile to use passphrase "1234567890123<>?=+&% The quick brown fox jumps over the lazy dog":

```
MX# set service-profile sp3 psk-phrase "1234567890123<>?=+&% The quick brown fox jumps over
    the lazy dog"
success: change accepted.
```

See Also

- **set mac-user attr** on page 9-177
- **set service-profile auth-psk** on page 12-284
- **set service-profile psk-raw** on page 12-296
- **set service-profile wpa-ie** on page 12-314
- **show service-profile** on page 12-347

set service-profile psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax **set service-profile** *profile-name* **psk-raw** *hex*

profile-name	Service profile name.
hex	A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults None.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage MSS converts the hexadecimal number into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the MX configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable WPA IE.

Examples The following command configures service profile to use a raw PSK with PSK clients:

```
MX# set service-profile sp3 psk-raw
    c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
```

```
success: change accepted.
```

See Also

- **set mac-user attr** on page 9-177
- **set service-profile auth-psk** on page 12-284
- **set service-profile psk-phrase** on page 12-295
- **set service-profile wpa-ie** on page 12-314
- **show service-profile** on page 12-347

set service-profile rsn-ie

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN (sometimes called WPA2) authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax **set service-profile** *profile-name* **rsn-ie** {**enable** | **disable**}

profile-name	Service profile name.
enable	Enables the RSN IE.
disable	Disables the RSN IE.

Defaults Disabled.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage When the RSN IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Examples The following command enables the RSN IE in service profile :

```
MX# set service-profile sprsn rsn-ie enable
success: change accepted.
```

See Also

- **set service-profile auth-dot1x** on page 12-282
- **set service-profile auth-psk** on page 12-284
- **set service-profile cipher-ccmp** on page 12-287
- **set service-profile cipher-wep104** on page 12-288
- **set service-profile cipher-wep40** on page 12-289
- **show service-profile** on page 12-347

set service-profile shared-key-auth

Enables shared-key authentication, in a service profile.

Syntax **set service-profile**

set service-profile soda agent-directory

Specifies the directory on the MX where the SODA agent files for a service profile are located.

Syntax **set service-profile** *profile-name* **soda agent-directory** *directory*

Defaults By default, the MX expects SODA agent files to be located in a directory with the same name as the service profile.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage If the same SODA agent is used

In order for the client to load the success page, you must make sure the SODA agent is cont-6(SOD -1A).a13.5361

set service-profile soda logout-page

Specifies a page on the MX switch that is loaded when a client logs out of the network by closing the SODA virtual desktop.

Syntax **set service-profile** *profile-name* **soda logout-page** *page*

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage When a client closes the SODA virtual desktop, the client is automatically disconnected from the network. You can use this command to specify a page that loads when the client closes the SODA virtual desktop.

The client can request this page at any time, to ensure that the client session is terminated. You can add the MX IP address to the DNS server as a well-known name, and you can advertise the URL of the page to users as a logout page.

The page is assumed to reside in the root directory on the MX. You can optionally specify a different directory where the page resides.

Note that you must also enable the HTTPS server on the MX, so that clients can log out of the network and access the logout page using HTTPS. To do this, use the **set ip https server enable** command.

Examples The following command specifies as the page to load when a client closes the SODA virtual desktop:

```
MX# set service-profile sp1 soda logout-page logout.html
success: change accepted.
```

The following command specifies , in the directory,7Is

History

Version 3.0	Command introduced
Version 4.0	Support added for blank spaces in the SSID name.

Examples The following command applies the name to the SSID managed by service profile :

```
MX# set service-profile clear_wlan ssid-name guest
success: change accepted.
```

The following command applies the name to the SSID managed by service profile :

```
MX# set service-profile mycorp_srvcprf ssid-name “corporate users”
success: change accepted.
```

See Also

- **set service-profile ssid-type** on page 12-304
- **show service-profile** on page 12-347

set service-profile ssid-type

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

Syntax **set service-profile** *profile-name* **ssid-type** [**clear** | **crypto**]

profile-name	Service profile name.
clear	Wireless traffic for the service profile's SSID is not encrypted.
crypto	Wireless traffic for the service profile's SSID is encrypted.

Defaults The default SSID type is crypto.

Access Enabled.

History Introduced in MSS Version 3.0.

Examples The following command changes the SSID type for service profile to **clear**:

```
MX# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

See Also

- **set service-profile ssid-name** on page 12-303
- **show service-profile** on page 12-347

set service-profile static-cos

Enables or disables static CoS on a service profile. Static CoS assigns the same CoS level to all traffic on the service profile SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any ACLs that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic.

When static CoS is enabled, the standard MSS prioritization mechanism is not used. Instead, the MP sets CoS as follows:

- For traffic from the MP to clients, the MP places the traffic into the forwarding queue that corresponds to the CoS level configured on the service profile. For example, if the static CoS level is set to 7, the MP radio places client traffic in its Voice queue.
- For traffic from clients to the network, the MP marks the DSCP value in the IP headers of the tunnel packets used to carry the user data from the MP to the MX.

Syntax **set service-profile** *profile-name* **static-cos** {**enable** | **disable**}

Defaults Static CoS is disabled by default.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage The CoS level is specified by the s**et service-profile cos** command.

Examples The following command enables static CoS on service profile :

```
MX# set service-profile sp1 static-cos enable
success: change accepted.
```

See Also

- **set service-profile cos** on page 12-289
- **show service-profile** on page 12-347

set service-profile tkip-mc-time

Changes the length of time that MP radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, MP radios dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

Syntax **set service-profile** *profile-name* **tkip-mc-time** *wait-time*

Defaults The default countermeasures wait time is 60,000 ms (60 seconds).

Access Enabled.

History Introduced in MSS Version 3.0.

Usage Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients

See Also

- **set service-profile cipher-tkip** on page 12-287
- **set service-profile wpa-ie** on page 12-314
- **show service-profile** on page 12-347

set service-profile transmit-rates

Changes the data rates supported by MP radios for a service-profile SSID.

Syntax **set service-profile** *profile-name* **transmit-rates** {**11a** | **11b** | **11g | 11na | 11ng**} **mandatory** *rate-list* [**disabled** *rate-list*] [**beacon-rate**

- **multicast-rate**—**auto** for all radio types.

Access Enabled.

History

History

Usage If you disable a rate, you cannot use the rate as a mandatory rate or the beacon or multicast rate. All rates that are applicable to the radio type and that are not disabled are supported by the radio.

Examples The following command sets 802.11a mandatory rates for service profile to 6 Mbps and 9 Mbps, disables rates 48 Mbps and 54 Mbps, and changes the beacon rate to 9 Mbps:

```
MX# set service-profile sp1 transmit-rates 11a mandatory 6.0,9.0 disabled 48.0,54.0
    beacon-rate 9.0
```

set service-profile user-idle-timeout

Changes the number of seconds MSS has a session available for a client not sending data and is not responding to keepalives (idle-client probes). If the timer expires, the client session is changed to the Dissociated state.

The timer is reset to 0 each time a client sends data or responds to an idle-client probe. If the idle-client probe is disabled, the timer is reset each time the client sends data.

Syntax **set service-profile** *profile-name* **user-idle-timeout** *seconds*

profile-name	Service profile name.
seconds	Number of seconds a client is allowed to remain idle before MSS changes the session to the Dissociated state. You can specify from 20 to 86400 seconds. To disable the timer, specify 0.

Defaults The default user idle timeout is 180 seconds (3 minutes).

Access Enabled.

History Introduced in MSS Version 4.2.

Examples The following command increases the user idle timeout to 360 seconds (6 minutes):

```
MX# set service-profile sp1 user-idle-timeout 360
success: change accepted.
```

See Also

- **set service-profile idle-client-probing** on page 12-290
- **set service-profile web-portal-session-timeout** on page 12-311
- **show service-profile** on page 12-347

set service-profile web-portal-acl

Changes the ACL name MSS uses to filter Web-Portal user traffic during authentication.

Use this command if you create a custom Web-Portal ACL to allow more than just DHCP traffic during authentication. For example, if you configure an ACL that allows a Web-Portal user to access a credit card server, this command uses the custom ACL for Web-Portal users that associate with the service profile SSID.

Syntax **set service-profile** *profile-name* **web-portal-acl** *aclname*

profile-name	Service profile name.
aclname	Name of the ACL to use for filtering Web-Portal user traffic during authentication.

Defaults By default, a service profile **web-portal-acl** option is unset. However, when you change the service profile **auth-fallthru** option to **web-portal**, MSS sets the **web-portal-acl** option to . (MSS automatically creates the ACL the first time you set any service profile **auth-fallthru** option to **web-portal**.)

Access Enabled.

History Introduced in MSS Version 5.0.

Usage The first time you set the service profile **auth-fallthru** option to **web-portal**, MSS sets the **web-portal-acl** option to . The value remains even if you change the **auth-fallthru** option again. To change the **web-portal-acl** value, you must use the **set service-profile web-portal-acl** command.

The Web-Portal ACL applies only to users who log on using Web-Portal, and applies only during authentication. After a Web-Portal user is authenticated, the Web-Portal ACL no longer applies. ACLs and other user attributes assigned to the username are applied instead.

Examples The following command changes the Web-Portal ACL name to on service profile to :

```
MX# set service-profile sp3 web-portal-acl creditsrvr
success: change accepted.
```

See Also

- **set service-profile auth-fallthru** on page 12-283
- **show service-profile** on page 12-347

set service-profile web-portal-form

Specifies a custom login page that loads for WebAAA users requesting the SSID managed by the service profile.

Syntax **set service-profile** *profile-name* **web-portal-form** *url*

Defaults The Trapeze Networks Web login page is served by default.

Access Enabled.

History

Usage It is recommended that you create a subdirectory for the custom page and place all of the files for the page in that subdirectory. Do not place the custom page in the root directory of the MX user file area.

If the custom login page includes gif or jpg images

```
MX# mkdir corpa
success: change accepted.

MX# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

MX# copy tftp://10.1.1.1/corpa-logo.jpg corpa/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]

MX# dir corpa
================================================================================
file:
Filename                                    Size           Created
file:corpa-login.html                       637 bytes   Aug 12 2004, 15:42:26
file:corpa-logo.jpg                        1202 bytes   Aug 12 2004, 15:57:11
Total:        1839 bytes used, 206577 Kbytes free

MX# set service-profile corpa-service web-portal-form corpa/corpa-login.html
success: change accepted.
```

See Also

- **copy** on page 21-485
- **dir** on page 21-488
- **mkdir** on page 21-492
- **set port type wired-auth** on page 5-58
- **set service-profile auth-fallthru** on page 12-283
- **set web-portal** on page 9-189
- **show service-profile** on page 12-347

set service-profile web-portal-logout logout-url

Specifies the URL that is requested when the user terminates a session in the Mobility Domain.

Syntax **set service-profile** *profile-name* **web-portal-logout logout-url** *url*

profile-name	Service profile name.
url	Specifies the URL for the Web Portal logout feature. The URL should be of the form **https://***host***/logout.html**.

Defaults By default, the logout URL uses the IP address of the MX as the part of the URL. The can be either an IP address or a hostname.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage Specifying the URL for the Web Portal logout feature is useful if you want to standardize the URL across your network. For example, you can configure the logout URL on all of the MX switches in the Mobility Domain as , where resolves to one of the MX switches in the Mobility Domain, ideally the seed.

To log out of the network, the user can click End Session in the window, or request the logout URL directly.

Standardizing the logout URL serves as a backup means for the user to log out in case the pop-under window is closed inadvertently. Note that if a user requests the logout URL, he or she must enter a username and password in order to identify the session on the MX. The username and password are both required to identify the session. If there is more than one session with the same username, then requesting the logout URL does not end any session.

Examples The following command configures the Web Portal logout URL as for service profile .

```
MX# set service-profile sp1 web-portal-logout logout-url https://wifizone.trpz.com/logout.html
success: change accepted.
```

See Also

- **set service-profile web-portal-logout mode** on page 12-311
- **show service-profile** on page 12-347

set service-profile web-portal-logout mode

Enables the Web Portal logout functionality, so that a user can manually terminate his or her session.

Syntax **set service-profile** *profile-name* **web-portal-logout mode** {**enable** | **disable**}

profile-name	Service profile name.
enable	Enables the Web Portal logout functionality
disable	Disables the Web Portal logout functionality.

Defaults Disabled.

Access Enabled.

History Introduced in MSS Version 6.0.

Usage When Web Portal logout functionality is enabled, after a Web Portal WebAAA user is successfully authenticated and redirected to the requested page, a pop-under window appears behind the user's browser. The window contains a button labeled "End Session". When the user clicks this button, a URL is requested that terminates the user's session in the Mobility Domain.

This feature allows Web Portal users a way to manually log out of the network, instead of automatically logging out when the Web Portal WebAAA session timeout period expires.

Examples The following command enables the Web Portal logout functionality for service profile .

```
MX# set service-profile sp1 web-portal-logout mode enable
success: change accepted.
```

See Also

- **set service-profile web-portal-logout logout-url** on page 12-310
- **show service-profile** on page 12-347

set service-profile web-portal-session-timeout

Changes the number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically.

Syntax **set service-profile** *name* **web-portal-session-timeout** *seconds*

name	Service profile name.
seconds	Number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically. You can specify from 5 to 2800 seconds.

Defaults The default Web Portal WebAAA session timeout is 5 seconds.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage When a client that has connected through Web Portal WebAAA enters standby or hibernation mode, the client may be idle for longer than the User idle-timeout period. When the User idle-timeout period expires, MSS places the client Web Portal WebAAA session in the Deassociated state. The Web Portal WebAAA session can remain in the Deassociated state for a configurable amount of time before being terminated automatically. This configurable amount of time is called the Web Portal WebAAA session timeout period. You can use this command to set the number of seconds in the Web Portal WebAAA session timeout period.

Note that the Web Portal WebAAA session timeout period applies only to Web Portal WebAAA sessions already authenticated with a username and password. For all other Web Portal WebAAA sessions, the default Web Portal WebAAA session timeout period is the number specified in the MSS Version 4.2.

set service-profile wep active-unicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

Syntax **set service-profile** *profile-name* **wep active-unicast-index** *num*

Defaults If WEP encryption is enabled and WEP keys are defined, MP radios use WEP key 1 to encrypt unicast frames, by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage Before using this command, you must configure values for the WEP keys you plan to use.

Examples The following command configures a 5-byte WEP key for key index 1 on service profile to :

```
MX# set service-profile sp2 wep key-index 1 key aabbccddee
success: change accepted.
```

See Also

- **set service-profile wep active-multicast-index** on page 12-312
- **set service-profile wep active-unicast-index** on page 12-313
- **show service-profile** on page 12-347

set service-profile wpa-ie

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax **set service-profile** *profile-name* **wpa-ie** {**enable** | **disable**}

profile-name	Service profile name.
enable	Enables the WPA IE.
disable	Disables the WPA IE.

Defaults Disabled.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites supported by the radios.

Examples The following command enables the WPA IE in service profile :

```
MX# set service-profile sp2 wpa-ie enable
success: change accepted.
```

See Also

- **set service-profile auth-dot1x** on page 12-282
- **set service-profile auth-psk** on page 12-284
- **set service-profile cipher-ccmp** on page 12-287
- **set service-profile cipher-tkip** on page 12-287
- **set service-profile cipher-wep104** on page 12-288
- **set service-profile cipher-wep40** on page 12-289
- **show service-profile** on page 12-347

show ap 11n-counters

Displays 802.11n statistics for 802.11n MPs.

Syntax show ap 11n-counters [*apnum* | radio [1 | 2]]

Defaults None

Access Enabled

History Introduced in MSS Version 7.0.

Usage Displays channel width, data rates, HT modes, and Ethernet links for 802.11n MPs.

Examples Use the following command to display 802.11n statistics for all 802.11n MPs or a single 802.11n radio.

```
MX# show ap 11n-counters 3 radio 1
AP: 9980              radio: 1
================================

Packet stats:
Tx packets count:        999002    Rx packets count:        999001
40MHz Tx packets count:  999004    40MHz Rx packets count:  999003
Tx packets retry count:  999005

Client stats:
Asscіated clients:       999006    11n clients:             999007
Powersave clients:       999008    SM powersave clients:    999009

Frame aggregation stats:
A-MSDU Tx count:         999011    A-MPDU Tx count:         999017
A-MSDU Rx count:         999010    A-MPDU Rx count:         999016
A-MSDU Tx frame count:   999013    A-MPDU Tx frame count:   999019
A-MSDU Rx frame count:   999012    A-MPDU Rx frame count:   999018
A-MSDU retry count:      999014    A-MPDU retry count:      999020
Compound aggregates:     999022

size(bytes)    <=4k       <=8k       <=16k      <=32k      <=64k   |    Peak
-----------  ---------- ---------- ---------- ---------- ---------- - ----------
A-MPDU Tx:  999026     999030     999034     999038     999042     | 999046
A-MPDU Rx:  999025     999029     999033     999037     999041     | 999045
A-MSDU Tx:  999024     999028     999032     999036     999040     | 999044
A-MSDU Rx:  999023     999027     999031     999035     999039     | 999043

subframes      <=4k       <=8k       <=16k      <=32k      <=64k   |    Peak
-----------  ---------- ---------- ---------- ---------- ---------- - ----------
A-MPDU Tx:  999050     999054     999058     999062     999066     | 999070
A-MPDU Rx:  999049     999053     999057     999061     999065     | 999069
A-MSDU Tx:  999048     999052     999056     999060     999064     | 999068
A-MSDU Rx:  999047     999051     999055     999059     999063     | 999067
```

Packet stats	❑ Tx packets count —Number of packets sent ❑ Rx packets count — Number of packets received ❑ 40MHz Tx packets count — Number of packets sent on the 40 MHz channel ❑ 40MHz Rx packets count — Number of packets received on the 40 MHz channel ❑ Tx Packet Retry count — Number of packets resent
Client stats	❑ Associated clients — Number of clients on the radio ❑ 11n clients— Number of 11n clients ❑ Powersave clients— Number of clients configured for powersave mode ❑ SM powersave clients —
Frame Aggregation stats	❑ A-MSDU Tx count — Number of MSDU packets sent ❑ A-MSDU Rx count — Number of MSDU packets received ❑ A-MSDU Tx frame count — Number of MSDU frames sent ❑ A-MSDU Rx frame count — Number of MSDU frames received ❑ A-MSDU retry count — Number of MSDU packets resent ❑ A-MPDU Tx count — Number of MPDU packets sent ❑ A-MPDU Rx count — Number of MPDU packets received ❑ A-MPDU Tx frame count — Number of MPDU frames sent ❑ A-MPDU Rx frame count — Number of MPDU frames received ❑ Compound Aggregates — The number of aggregated packets
size	❑ A-MPDU Tx count — Number of MSDU packets sent ❑ A-MPDU Rx count — Number of MSDU packets received ❑ A-MSDU Tx count — Number of MPDU packets sent ❑ A-MSDU Rx count — Number of MPDU packets received ❑ Peak — The largest size packet sent or received.

show ap acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the specified MP if the MP is configured to perform local switching. Each time a packet is filtered by a security ACL, the MP ACL hit counter increments.

Syntax **show ap acl hits** *apnum*

Defaults None.

Access Enabled.

History I

- **set security acl** on page 15-395

show ap acl resource-usage

Displays statistics about the resources used by security ACL filtering on the MP.

Syntax **show ap acl resource-usage** *apnum*

apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.

Defaults None.

Access Enabled.

History

Version 6.0	Command introduced.
Version 6.2	Added index value range from 1 to 9999.

Usage Use this command with the help of the Trapeze Technical Assistance Center (TAC) to diagnose an ACL resource problem.

Examples To display security ACL resource usage for MP 7, type the following command:

```
MX# show ap acl resource-usage 7
AP 7 mapped ACL counters
-----------------------------------------

  Number of rule groups   :          0
  Number of rules         :          0
  Number of maps          :          0
```

show ap arp

Displays the ARP table for a specified MP.

Syntax **show ap arp** *apnum*

apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.

Defaults None.

Access All.

History

Version 6.0	Command introduced.
Version 6.2	Added index value range from 1 to 9999.

Examples The following command displays ARP entries for AP 7:

```
MX# show ap arp 7
AP 7:
Host                          HW Address        VLAN  State    Type
----------------------------- ----------------- ----- -------- -------
10.5.4.51                     00:0b:0e:00:04:0c     1 EXPIRED  DYNAMIC
```

```
10.5.4.53                    00:0b:0e:02:76:f7     1 RESOLVED LOCAL
```

Table 13 describes the fields in this display.

See Also

- **set ap local-switching mode** on page 12-242
- **set vlan-profile** on page 6-75

show ap config

Displays a summary of MPs configured on your network.

show ap config radio

Displays global and radio-specific settings for an MP.

Syntax **show ap** *apnum* **config** [*port-list* [**radio** {**1**

```
      contact:
Radio 1: type: 802.11g, mode: disabled, channel: dynamic
tx pwr: 18, profile: default
auto-tune max-power: default,
load-balance-group: ,
load-balance-enable: YES,
force-rebalance: NO,
local-switching: disabled, vlan-profile: default
```

Table 12– 1 describes the fields in this display.

Port	MX port number to which the MP is connected, if specified for the MP.
AP	Index number that identifies the MP on the MX.
serial-id	Serial number on the MP.
AP model	MP model number.
bias	Bias of the MX connection to the MP: ❑ High ❑ Low
name	MP access point name, if configured.
upgrade-firmware	State of the firmware upgrade option: ❑ YES (automatic upgrades are enabled) ❑ NO (automatic upgrades are disabled)
force-image-download	State of the option to force the MP to download a software image from the MX instead of loading a locally stored image on the MP.
communication timeout	
location	Location information for the MP.
contact	Contact information for the MP.
Radio	Radio number. The information listed below this field applies specifically to the radio.
type	Radio type: ❑ 802.11a ❑ 802.11b ❑ 802.11g
mode	Radio state: ❑ Enabled ❑ Disabled
channel	Channel number.
antennatype	External antenna model, if applicable.
tx pwr	Transmit power, in dBm.
profile	Radio profile that manages the radio. Until you assign the radio to a radio profile, MSS assigns the radio to the default radio profile.
auto-tune max-power	Maximum power level the RF Auto-Tuning feature can set on the radio. ❑ The value means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation. ❑ A specific numeric value means you or another administrator set the maximum value.

See Also

- **set ap** on page 5-51
- **set port type ap** on page 5-58
- **set ap bias** on page 12-232
- **set ap fingerprint** on page 12-240
- **set ap group** on page 12-241
- **set ap name** on page 12-243
- **set ap upgrade-firmware** on page 12-253
- **set ap radio mode** on page 12-249
- **set ap radio antennatype** on page 12-244
- **set ap radio channel** on page 12-246
- **set ap radio radio-profile** on page 12-251
- **set ap radio tx-power** on page 12-251
- **show ap connection** on page 12-339
- **show ap global** on page 12-341
- **show ap w⌈show ap w⌈show ap w⌈show a-41)4c-.0002 Tw⌈show ap w⌈show ap w⌈show ap w⌈show a**

History

Version 1.0 Command introduced.

Usage To display statistics counters and other information for individual user sessions, use the **show sessions network** command.

Examples The following command shows statistics counters for Distributed MP 7:

```
MX# show ap counters 7

AP: 7                radio: 1
================================
LastPktXferRate        2         PktTxCount         73473
NumCntInPwrSave        0         MultiPktDrop       0
LastPktRxSigStrength   -89       MultiBytDrop       0
LastPktSigNoiseRatio   4         User Sessions      0
TKIP Pkt Transfer Ct   0         MIC Error Ct       0
TKIP Pkt Replays       0         TKIP Decrypt Err   0
CCMP Pkt Decrypt Err   0         CCMP Pkt Replays   0
CCMP Pkt Transfer Ct   0         RadioResets        0
Radio Recv Phy Err Ct  0         Transmit Retries   60501
Radio Adjusted Tx Pwr  15        Noise Floor        -93
802.3 Packet Tx Ct     0         802.3 Packet Rx Ct 0
No Receive Descriptor  0         Illegal Rates      2
```

Radio Adjusted Tx Pwr	Current power level set on the radio. If RF Auto-Tuning of power is enabled, this value is the power set by RF Auto-Tuning. If RF Auto-Tuning is disabled, this value is the statically configured power level.
802.3 Packet Tx Ct	Number of raw 802.3 packets transmitted by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.
No Receive Descriptor	Number of packets for which the MP could not create a descriptor. A descriptor describes a received packet's size and its location in MP memory. The MP buffers descriptors, and clears them during interframe spaces. This counter increments if the MP runs out of buffers for received packets. This condition can occur when a noise burst temporarily floods the air and the MP attempts to buffer the noise as packets. Buffer overruns are normal while an MP is booting. However, if they occur over an extended period of time when the MP is fully active, this can indicate RF interference.
Illegal Rates	Number of times a client attempted to connect with a disabled data rate.
PktTxCount	Number of packets transmitted by the radio.
MultiPktDrop	Number of multicast packets dropped by the radio due to a buffer overflow on the MP. This counter increments if there is too much multicast traffic or there is a problem with the multicast packets. Normally, this counter should be 0.
MultiBytDrop	Number of multicast bytes dropped by the radio due to a buffer overflow on the MP. (See the description for MultiPktDrop.)
User Sessions	Number of clients currently associated with the radio. Generally, this counter is equal to the number of sessions listed for the radio in **show sessions** output. However, the counter can differ from the counter in

Noise Floor	Received signal strength at which the MP can no longer distinguish 802.11 packets from ambient RF noise. A value around -90 or higher is good for an 802.11b/g radio. A value around -80 or higher is good for an 802.11a radio. Values near 0 can indicate RF interference.
802.3 Packet Rx Ct	Number of raw 802.3 packets received by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.

The counters above are global for all data rates. The counters below are for individual data rates.

Note: If counters for lower data rates are incrementing but counters for higher data rates are not incrementing, this can indicate poor throughput. The poor throughput can be caused by interference. If the cause is not interference or the interference cannot be eliminated, you might need to relocate the MP in order to use the higher data rates and therefore improve throughput.

TxUniPkt	Number of unicast packets transmitted by the radio.
TxMultiPkt	Number of multicast packets transmitted by the radio.
TxUniByte	Number of unicast bytes transmitted by the radio.
TxMultiByte	Number of multicast bytes transmitted by the radio.
RxPkt	Number of packets received by the radio.
RxByte	Number of bytes received by the radio.
UndcrptPkt	Number of undecryptable packets received by the radio. It is normal for this counter to increment even in stable networks and does not necessarily indicate an attack. For example, a client might be sending incorrect key information. However, if the counter increments rapidly, there might be a problem in the network.
UndcrptByte	Number of undecryptable bytes received by the radio. (See the description for UndcrptPkt.)
PhyError	Number of packets that could not be decoded by the MP. This condition can have any of the following causes: ❑ Collision of an 802.11 packet. ❑ Packet whose source is too far away, thus rendering the packet unintelligible by the time it reaches the MP.003 Tw[(problem in)6.7(the network.)53time e(et

See Also **show sessions network** on page 19-453

show ap fdb

Displays the entries in a specified MP forwarding database.

Syntax **show ap fdb** {*apnum* | **all | hash-utilization [***apnum* |**all]}**

Defaults None.

Access All.

History

Examples The following command displays FDB entries for AP 7:

```
MX# show ap fdb 7
AP 7:
# = System Entry. $ = Authenticate Entry
VLAN TAG  Dest MAC/Route Des [CoS] Destination Ports
---- ---- ----------------- ----- ----------------
4095 4095 00:0b:0e:00:ca:c1      #          CPU
4095    0 00:0b:0e:00:04:0c                eth0
```

Table 12– 3 describes the fields in the **show ap fdb** output.

See Also

- **set ap local-switching mode** on page 12-242

Usage Repeating this command with the **clear** option at regular intervals allows you to monitor transmission and drop rates.

Examples The following command shows statistics for the MP forwarding queues on a Distributed MP:

```
MX# show ap qos-stats 7
CoS  Queue       Rx      Rx      Tx      Tx    Tx    Tx    Tx          Tx
                 Kbs     %       Kbs     %     %Req  %Max  Packets     Dropped
==============================================================================
    AP: 7  radio: 1
1,2  Background        0     0         0     0     0     0           0        0
0,3  BestEffort       93     9         0     0     0     0           0        0
4,5  Video             0     0         0     0     0     0           0        0
6,7  Voice             0     0         0     0     0     0           0        0
    AP: 7  radio: 2
1,2  Background        0     0         0     0     0     0           0        0
0,3  BestEffort      127     3         0     0     0     0           0        0
4,5  Video             0     0         0     0     0     0           0        0
6,7  Voice             0     0         0     0     0     0           0        0
```

Table 12– 4 describes the fields in this display.

show ap etherstats

Displays Ethernet statistics for an Ethernet port on an MP.

Syntax **show ap etherstats** *apnum*

Defaults None.

Access Enabled.

show ap group

Deprecated in MSS Version 6.0. To display information about RF load balancing, see **show load-balancing group** on page 12-343.

show ap mesh-links

Displays information about the links an MP has to Mesh APs and Mesh Portal APs.

Syntax **show aph.hs.h-.h** ap-h

AP	Identifier for the MP on the MX.
Name	VLAN name
IP-addr	IP address of the MP.
Operational Mode	If this MP is a Mesh AP or a Mesh Portal AP
Downlink Mesh-APs	Information about the Mesh APs associated with the Mesh Portal MP.
BSSID	The BSSID of the Mesh AP.

See Also

- **set ap boot-configuration mesh ssid** on page 12-237
- **set service-profile mesh** on page 12-293

show ap status

Displays MP access point and radio status information.

Syntax **show ap status** [**terse**] | [*apnum* | **all** [**radio** {**1** | **2**}]]

Defaults None.

Access Enabled.

History

Version 4.0	❑ New option added: **terse** ❑ New option added for **show dap status**: **all** ❑ New field added: fingerprint ❑ MP-MX security status added to State field **Note:** The fingerprint field and security state apply to the display for Distributed MPs only.
Version 4.1	❑ External antenna information added after the radio state information, to indicate when an antenna has been detected and to indicate the confiS (e)-2. (e)12.er th

V. Tm0 Tc0 Tw()Tj/TT6 1 Tf9 0 0 0688.02 Tm-.0005 Tc12.0043 Tw[(Ex)-5(tern)0044((onl)-o002 Tc.004

Examples The following command displays the status of an MP access point:

```
MX# show ap status 9991
Flags: o = operational[0], c = configure[0], d = download[0], b = boot[0]
       a = auto AP, m = mesh AP, p/P = mesh portal (ena/actv), r = redundant[0]
       i = insecure, e = encrypted, u = unencrypted
Radio: E = enabled - 20MHz channel, S = sentry
       W/w = enabled - 40MHz wide channel (HTplus/HTminus)
       D = admin disabled
IP Address: * = AP behind NAT
AP   Flag IP Address      Model        MAC Address       Radio 1 Radio 2 Uptime
---- ---- -------------- ------------ ----------------- ------- ------- ------
9991 oa-i 129.0.1.10      MP-422       00:0b:0e:00:1b:00 E  6/22 D 44/18 03d21h
```

The following command uses the **verbose** option to display all information for MPs:

```
MX# show ap status verbose
```

```
Rack28-2800-112226# show ap status 9991 verbose
AP: 9991 Name: AUTO-9991
  Model: Trapeze MP-422, Rev: n/a, Serial number: 108
            F/W1 : 1.0
            F/W2 : 1.0
            S/W  : 7.0.1.0.private_032408_1529_jperson
       BOOT S/W  : <unknown>
  IP-addr: 129.0.1.10 (DHCP, vlan 'apboot'),
  Port 1 link: 10/Half , POE: 802.3af
  Port 2 link: down , POE: 802.3af
  State: operational (encrypted and fingerprint not verified)
```

```
( )-6( (( )-6( R )-6FID p)-6reUp)-6ortse:IpTa
```

AP	The index number of the connected MP
Name	The name of the MP.
Model	❑ MP model number ❑ Revision number ❑ Serial Number ❑ Firmware versions ❑ Software version ❑ Boot software version
IP Address	❑ IP address of the MP. The address is assigned to the MP by a DHCP server. ❑ VLAN assigned to the MP. **Note:** This field is applicable only if the MP is configured on the MX as a Distributed MP.

show ap vlan

Displays information about locally switched or tunneled VLANs.

Syntax **show ap vlan** *apnum*

apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
all	Displays all MPs on a VLAN.

Defaults None.

Access All.

History

Version 6.0	Command introduced.
Version 6.2	Introduced index value range of 1 to 9999.
Version 7.0	Added **all** option.

Examples The following command displays information about the VLANs switched by AP 7:

```
MX# show ap vlan 7
AP 7:
VLAN Name             Mode    Port              Tag
---- ---------------- ----    ---------------- ----
   1 default          local                  1 none
   2 red              local                  1    2
                                       radio_1   20
                                       radio_1   21
                                       radio_2   22
   4 green            local                  1    4
                                       radio_1   23
   5 yellow           tunnel          mx_tun    5
                                      radio_1   24
```

Table 12– 3 describes the fields in the **show ap vlan** output.

VLAN	VLAN number.
Name	VLAN name
Mode	Whether packets for the VLAN are locally switched by the MP, or are tunneled to an MX, which places them on the VLAN.
Port	The port(s) through which VLAN traffic is sent.
TAG	VLAN tag value. If the interface is untagged, none is displayed in the TAG field.

See Also

- **set ap local-switching mode** on page 12-242
- **set vlan-profile** on page 6-75

show auto-tune attributes

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

Syntax **show auto-tune attributes** [**ap** *apnum* [**radio** {**1** | **2**| **all**}]]

Defaults None.

Access

- **set radio-profile auto-tune channel-interval** on page 12-258
- **set radio-profile auto-tune power-config** on page 12-260
- **set radio-profile auto-tune power-interval** on page 12-261
- **show auto-tune neighbors** on page 12-337
- **show radio-profile** on page 12-344

show auto-tune neighbors

See Also

- **set ap radio auto-tune max-power** on page 12-245
- **set radio-profile auto**

IP Address:

Usage The **serial-id** parameter displays the active connection for the specified Distributed MP even if that MP is not configured on this MX. If you instead use the command with the parameter or without a parameter, connection information is displayed only for Distributed MPs configured on this MX.

This command provides information only if the Distributed MP is configured on the MX where you entered the command. The MX does not need to be the one that booted the MP, but it must have the MP in the configuration. Also, the MX that booted the MP must be in the same Mobility Domain as the MX where you entered the command.

If a Distributed MP is configured on this MX (or another MX in the same Mobility Domain) but does not have an active connection, the command does not display information for the MP. To show connection information for Distributed MPs, use the **show ap global** command on one of the switches where the MPs are configured.

Examples The following command displays information for all Distributed MPs configured on this MX switch that have active connections:

```
MX# show ap connection
Total number of entries: 2
AP Serial Id    AP IP Address  MX IP Address
--- ----------- -------------- --------------
2   112233      10.10.2.27     10.3.8.111
4   0333000298  10.10.3.34     10.3.8.111
```

The following command displays connection information specifically for a Distributed MP with serial ID :

```
MX# show ap connection serial-id 223344
Total number of entries: 1
AP Serial Id AP IP Address  MX IP Address
--- ----------- -------------- --------------
9   223344      10.10.4.88     10.9.9.11
```

Table 12– 13

show ap global

Displays connection information for Distributed MPs configured on an MX .

Syntax **show ap global** [*apnum* | **serial-id** *serial-ID*]

apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
serial-id *serial-ID*	MP access point serial ID.

Defaults None.

Access Enabled.

History

Version 2.0	Command introduced.
Version 6.0	Option **dap** removed.
Version 6.2	Added index value range from 1 to 9999.

Usage Connections are shown only for the Distributed MPs configured on the MX that you enter the command, and only for the Mobility Domain of the MX.

To show information only for Distributed MPs that have active connections, use the **show ap connection** command.

Examples The following command displays connection information for all the Distributed MPs configured on an MX:

```
MX# show ap global
Total number of entries: 8
AP Serial Id   MX IP Address   Bias
--- ----------- --------------- ----
1   11223344    10.3.8.111      HIGH
-   11223344    10.4.3.2        LOW
2   332211      10.3.8.111      LOW
-   332211      10.4.3.2        HIGH
17  0322100185  10.3.8.111      HIGH
-   0322100185  10.4.3.2        LOW
18  0321500120  10.3.8.111      LOW
-   0321500120  10.4.3.2        HIGH
```

Table 12– 14 describes the fields in this display.

AP	ID you assigned to the Distributed MP. **Note:** AP numbers are listed only for Distributed MPs configured on this MX switch. If the field contains a hyphen (-), the Distributed MP configuration displayed in the row of output is on another MX switch.
Serial Id	Serial ID of the Distributed MP.

MX IP Address	System IP address of the MX on which the Distributed MP is configured. A separate row of output is displayed for each MX on which the Distributed MP is configured.
Bias	Bias of the MX for the MP: ❑ High ❑ Low

See Also

- **set ap** on page 5-51
- **set ap bias** on page 12-232
- **show ap config radio** on page 12-320
- **show ap connection** on page 12-339
- **show ap unconfigured** on page 12-342

show ap unconfigured

Displays Distributed MPs that are physically connected to the network but that are not configured on any MX switches.

Syntax **show ap unconfigured**

Defaults None.

Access Enabled.

History

Version 2.0	Command introduced.
Version 6.0	Option **dap** removed.

Usage This command also displays an MP that is directly connected to an MX, if the MX port connected to the MP is configured as a network port instead of an MP access port, and if the network port is a member of a VLAN.

If a Distributed MP is configured on an MX, the MP can appear in the output until the MP is able to establish a connection with an MX in a Mobility Domain. After the MP establishes a connection, the entry for the MP ages out and no longer appears in the command output.

Entries in the command output table age out after two minutes.

Examples The following command displays information for two Distributed MPs that are not configured:

```
MX# show ap unconfigured
Total number of entries: 2
Serial Id   Model  IP Address      Port Vlan
----------- ------ --------------- ---- --------
0333001287  MP-241 10.3.8.54       5    default
0333001285  MP-252 10.3.8.57       7    vlan-eng
```

Table 12– 15 describes the fields in this display.

Serial Id	Serial ID of the MP.
Model	MP model number.
IP Address	IP address of the MP. This is the address that the MP receives from a DHCP server. The MP uses this address to send a Find MX message to request configuration information from MX switches. However, the MP cannot use the address to establish a connection unless the MP first receives a configuration from an MX.
Port	Port number on which this MX received the MP Find MX message.
VLAN	VLAN that this MX received the MP Find MX message.

See Also

- **show ap connection** on page 12-339
- **show ap global** on page 12-341

show load-balancing group

Displays an RF load balancing group's member radios and current load for each radio.

Syntax **show load-balancing group** {*group-name* | **all** | [**ap** *apnum* **radio** {**1** | **2**}]}

group-name	Name of an RF load-balancing group configured on the MX.
all	Displays information for every load-balancing group that has a radio on this MX as a member.
apnum	Index value that identifies the MP on the MX. You can specify a value from 1 to 9999.
radio {**1** | **2**}	Shows status information for a radio on an MP. This option displays information about radios in the same group as the specified radio.

Defaults None.

Access Enabled.

History

Version 6.0	Command introduced.

Usage Use this command to display information about the RF load-balancing groups configured on the MX and the individual MP radios in the load-balancing groups.

Examples The following command displays information about the MP radios that are in the same group as radio 1 on MP 3:

```
MX# show load-balancing group ap 3 radio 1
Radios in the same load-balancing group as: ap3/radio1
-----------------------------------------------
IP address         AP    Radio  Overlap
------------------ ----  -----  -------
       10.2.28.200    3      1  100/100
```

The following command displays information about RF load balancing group :

```
MX# show load-balancing group blue
Load-balancing group: blue
```

```
IP address          AP    Radio  Clients
------------------- ----  -----  -------
       10.2.28.200    3      1        0
```

Table 12– 16

Version 3.0
- Fields removed for items that are no longer managed by radio profiles:
  - Encrypted Network Name
  - Clear Network Name
  - Network name(s) broadcast in the wireless beacon
  - WEP Key 1 value
  - WEP Key 2 value
  - WEP Key 3 value
  - WEP Key 4 value
  - WEP Unicast Index
  - WEP Multicast Index
  - Shared Key Auth
  - WPA enabled

  These items are now managed by service profiles.
- New fields added:
  - Tune Channel
  - Tune Power
  - Tune Channel Interval
  - Tune Power Interval
  - Client Backoff Timer
  - Channel Holddown
  - Service profiles
- Name of the 802.11g field changed from Allow only 802.11g clients in 802.11g networks to Allow 802.11g clients only

Version 4.0
- New fields added:
  - Countermeasures
  - Active-Scan
  - WMM enabled
- Name of the backoff timer field changed from Client Backoff Timer to Power Backoff Timer

Version 4.2
- WMM enabled field renamed to QoS Mode.
- Long Retry Limit and Short Retry Limit fields moved to **show service-profile** output. (These options are now configurable on a service-profile basis instead of a radio-profile basis.)
- Allow 802.11g clients only field removed. (This option is now configured using the **set service-profile transmit-rates** command.)

Version 5.0
- New fields added:
  - Power ramp interval
  - RFID enabled
  - WMM Powersave
- Power Backoff Timer field removed.

Usage MSS contains a radio profile. Trapeze Networks recommends that you do not change this profile but instead keep the profile for reference.

Examples The following command shows radio profile information for the radio profile:

```
MX# show radio-profile default
Beacon Interval:                100   DTIM Interval:                   1
Max Tx Lifetime:               2000   Max Rx Lifetime:              2000
RTS Threshold:                 2346   Frag Threshold:               2346
Long Preamble:                   no   Tune Channel:                  yes
Tune Power:                      no   Tune Channel Interval:        3600
Tune Power Interval:            600   Power ramp interval:            60
Channel Holddown:               300   Countermeasures:              none
Active-Scan:                    yes   RFID enabled:                   no
WMM Powersave:                   no   QoS Mode:                      wmm

No service profiles configured.
```

Table 12– 17 describes the fields in this display.

Beacon Interval	Rate (in milliseconds) at which each MP radio in the profile advertises the beaconed SSID.
DTIM Interval	Number of times after every beacon that each MP radio in the radio profile sends a delivery traffic indication map (DTIM).
Max Tx Lifetime	Number of milliseconds that a frame by a radio in the radio profile can remain in buffer memory.
Max Rx Lifetime	Number of milliseconds that

Service profiles	Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID. **Note:** When you upgrade from 2.xAc5GE creates a default-dot1x service profile for encrypted SSIDs and a default-clear service profile for unencrypted SSIDs. These default service profiles contain the default encryption settings for crypto SSIDs and clear SSIDs, respectively.

See Also

- **set radio-profile active-scan** on page 12-256
- **set radio-profile auto-tune 11a-channel-range** on page 12-256
- **set radio-profile auto-tune channel-holddown** on page 12-258
- **set radio-profile auto-tune channel-interval** on page 12-258
- **set radio-profile auto-tune channel-lockdown** on page 12-259
- **set radio-profile auto-tune power-config** on page 12-260
- **set radio-profile auto-tune power-interval** on page 12-261
- **set radio-profile auto-tune power-lockdown** on page 12-261
- **set radio-profile auto-tune power-ramp-interval** on page 12-262
- **set radio-profile beacon-interval** on page 12-263
- **set radio-profile countermeasures** on page 12-265
- **set radio-profile dfs-channels** on page 12-265
- **set radio-profile frag-threshold** on page 12-267
- **set radio-profile max-rx-lifetime** on page 12-268
- **set radio-profile max-tx-lifetime** on page 12-268
- **set radio-profile mode** on page 12-269
- **set radio-profile preamble-length** on page 12-271
- **set radio-profile qos-mode** on page 12-272
- **set radio-profile rf-scanning mode** on page 12-274
- **set radio-profile rts-threshold** on page 12-275
- **set radio-profile service-profile** on page 12-275
- **set radio-profile wmm-powersave** on page 12-280

show service-profile

Displays service profile information.

Syntax **show service-profile** {*profile-name* | **?**}

profile-name	Displays information about the named service profile.
?	Displays a list of service profiles.

Defaults None.

Access Enabled.

History

Version 3.0	Command introduced
Version 4.1	New fields added to indicate the configured SSID default attributes in the service profile.
Version 4.2	New fields added: ❑ Proxy ARP ❑ DHCP restrict ❑ No broadcast ❑ Short retry limit (moved from **show radio-profile** output) ❑ Long retry limit (moved from **show radio-profile** output) ❑ Sygate On-Demand (SODA) ❑ Enforce SODA checks: ❑ SODA remediation ACL ❑ Custom success web-page ❑ Custom failure web-page ❑ Custom logout web-page ❑ Custom agent-directory ❑ Static COS ❑ COS ❑ CAC mode ❑ CAC sessions ❑ User idle timeout ❑ Idle client probing ❑ Web Portal Session Timeout ❑ Transmit rates for 11a / 11b / 11g: • beacon rate • multicast rate • mandatory rate • standard rates • disabled rates
Version 5.0	New fields added: ❑ Active call timeout ❑ Keep initial vlan ❑ Web Portal ACL
Version 6.0	New fields added: ❑ Client DSCP ❑ Mesh enabled ❑ Bridging enabled ❑ Load Balance Exempt ❑ Web Portal Logout ❑ Custom Web Portal Logout URL

Examples The following command displays information for service profile :

```
MX# show service-profile sp1
ssid-name:                      corp2    ssid-type:                    crypto
Beacon:                           yes   Proxy ARP:                       no
DHCP restrict:                     no   No broadcast:                    no
Short retry limit:                  5   Long retry limit:                 5
Auth fallthru:                   none   Sygate On-Demand (SODA):         no
Enforce SODA checks:              yes   SODA remediation ACL:
Custom success web-page:                Custom failure web-page:
Custom logout web-page:                 Custom agent-directory:
Static COS:                        no   COS:                              0
Client DSCP:                       no   CAC mode:                      none
CAC sessions:                      14   User idle timeout:              180
Idle client probing:              yes   Keep initial vlan:               no
```

```
Web Portal Session Timeout:          5   Mesh enabled:                       no
Web Portal ACL:                          Bridging enabled:                   no
Load Balance Exempt:                no   Web Portal Logout:                  no
Custom Web Portal Logout URL:
WEP Key 1 value:                <none>   WEP Key 2 value:                <none>
WEP Key 3 value:                <none>   WEP Key 4 value:                <none>
WEP Unicast Index:                   1   WEP Multicast Index:                 1
Shared Key Auth:                    NO
11a beacon rate:                   6.0   multicast rate:                   AUTO
11a mandatory rate: 6.0,12.0,24.0 standard rates: 9.0,18.0,36.0,48.0,54.0
11b beacon rate:                   2.0   multicast rate:                   AUTO
11b mandatory rate: 1.0,2.0 standard rates: 5.5,11.0
11g beacon rate:                   2.0   multicast rate:                   AUTO
11g mandatory rate: 1.0,2.0,5.5,11.0 standard rates: 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
```

Table 12– 18 describes the fields in this display.

ssid-name	Service set identifier (SSID) managed by this service profile.
ssid-type	SSID type: ❑ crypto—Wireless traffic for the SSID is encrypted. ❑ clear—Wireless traffic for the SSID is unencrypted.
Beacon	Indicates whether the radio sends beacons, to advertise the SSID: ❑ no ❑ yes
Proxy ARP	Indicates whether proxy ARP is enabled. When this feature is enabled, MSS answers ARP requests on behalf of wireless clients.
DHCP restrict	Indicates whether DHCP Restrict is enabled. When this feature is enabled, MSS allows only DHCP traffic for a new client until the client has successfully completed authentication and authorization.
No broadcast	Indicates if broadcast restriction is enabled. When this feature is enabled, MSS sends ARP requests and DHCP Offers and Acks as unicasts to their target clients instead of forwarding them as broadcasts.
Short retry limit	Number of times a radio serving the service-profile's SSID can send a short unicast frame without receiving an acknowledgment.
Long retry limit	Number of times a radio serving the service-profile SSID can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is the RTS threshold.
Auth fallthru	Secondary (fallthru) encryption type when a user tries to authenticate but the MX managing the radio does not have an authentication rule with a userglob that matches the username. ❑ last-resort—Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password. ❑ none—Denies authentication and prohibits the user from accessing the SSID. ❑ web-portal—Redirects the user to a web page for login to the SSID.
Sygate On-Demand (SODA)	Whether SODA functionality is enabled for the service profile. When SODA functionality is enabled, connecting clients download SODA agent files, which perform security checks on the client.
Enforce SODA checks	If a client is allowed access to the network after it has downloaded and run the SODA agent security checks. When SODA functionality is enabled, and the MX is configured to enforce SODA checks, then a connecting client must download the SODA agent files and pass the checks in order to gain access to the network.

SODA remediation ACL	The name of the ACL to be applied to the client if it fails the SODA agent checks. If no remediation ACL is specified, then a client is disconnected from the network if it fails the SODA agent checks.
Custom success web-page	The name of the user-specified page that the client loads upon successful completion of the SODA agent checks. If no page is specified, then the success page is generated dynamically.
Custom failure web-page	The name of the user-specified page that the client loads if it fails SODA agent checks. If no page is specified, then the failure page is generated dynamically.
Custom logout web-page	The name of the user-specified page that the client loads upon logging out of the network, either by closing the SODA virtual desktop, or by requesting the page. If no page is specified, then the client is disconnected without loading a logout page.
Custom agent-directory	The name of the directory for SODA agent files on the MX switch, if different from the default. By default, SODA agent files are stored in a directory with the same name as the service profile.
Static COS	Indicates whether static CoS assignment is enabled. When this feature is enabled, MPs assign the CoS value in the COS field to all user traffic forwarded by the MP.
COS	CoS value assigned by the MP to all user traffic, if static CoS is enabled. (If static CoS is disabled, WMM or ACLs are used to assign CoS.)
Client DSCP	If packets are classified based on client DSCP level instead of 802.11 priority.
CAC mode	Call Admission Control mode: ❑ none—CAC is disabled. ❑ session—CAC is based on the number of active user sessions. If an MP radio reaches the maximum number of active user sessions specified in the CAC session field, the MP radio rejects new connection attempts.
CAC sessions	Maximum number of user sessions that can be active on an MP radio at one time, if the CAC mode is session. (If the CAC mode is none, this value is not used.)
User idle timeout	Indicates how many seconds a user session can remain idle (indicated by no user traffic and no reply to client keepalive probes) before the session is changed to the Disassociated state.
Idle client probing	Indicates whether client keepalive probes are enabled.
Keep initial VLAN	Indicates whether the **keep-initial-vlan** option is enabled.
Web Portal Session Timeout	When a Web Portal WebAAA session is placed in the Deassociated state, how many seconds the session can remain in that state before being terminated automatically.
Mesh enabled	Whether WLAN mesh services are enabled for the service profile.
Web Portal ACL	Name of the ACL used to filter traffic for Web Portal users associated with this service profile's SSID while the users are being authenticated.
Bridging enabled	If wireless bridging is enabled for this service profile.
Load Balance Exempt	If the MP radios managed by this service profile are exempted (do not participate in) RF load balancing.
Web Portal Logout	If the Web Portal WebAAA logout functionality has been enabled.
Custom Web Portal Logout URL	If configured, the URL that Web Portal WebAAA users can access in order to terminate their sessions.

WEP Key 1 value	State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-Equivalent Privacy (WEP): ❑ none—The key is not configured. ❑ preset—The key is configured. **Note:** The WEP parameters apply to traffic only on the encrypted SSID.
WEP Key 2 value	State of static WEP key number 2: ❑ none—The key is not configured. ❑ preset—The key is configured.
WEP Key 3 value	State of static WEP key number 3: ❑ none—The key is not configured. ❑ preset—The key is configured.
WEP Key 4 value	State of static WEP key number 4: ❑ none—The key is not configured. ❑ preset—The key is configured.
WEP Unicast Index	Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID.
WEP Multicast Index	Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID.
Shared Key Auth	Indicates whether shared-key authentication is enabled.
WPA enabled or RSN enabled	Indicates that the Wi-Fi Protected Access (WPA) or Robust Security Network (RSN) information element (IE) is enabled. Additional fields displa0041 Tw[(RS)-ym17..e tler

show service-profile cac session

Displays current session counts on all MPs using the specified service profile, when session-based CAC is enabled.

Syntax **show service-profile** *profile-name* **cac session**

profile-name TD0 T

Defaults None.

Access Enabled.

History Introduced in MSS Version 6.0.

Examples The following command displays information about session counts for service profile :

```
MX# show service-profile sp1 cac session
Service Profile   sp1
CAC Mode          SESSION
Max Sessions      14
```

Table 12– 19

Use Spanning Tree Protocol (STP) commands to configure and manage spanning trees on the virtual LANs (VLANs) configured on an MX, to maintain a loop-free network. This chapter presents STP commands alphabetically. Use the following table to locate commands in this chapter based on their use.

clear spantree portcost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge in all VLANs on an MX.

Syntax **clear spantree portcost** *port-list*

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage This command resets the cost in all VLANs. To reset the cost for only specific VLANs, use the **clear spantree portvlancost** command.

Examples The following command resets the STP port cost on ports 5 and 6 to the default value:

```
MX# clear spantree portcost 5-6
success: change accepted.
```

See Also

- **clear spantree portvlancost** on page 13-357
- **set spantree portcost** on page 13-360
- **set spantree portvlancost** on page 13-362
- **show spantree** on page 13-364
- **show spantree portvlancost** on page 13-368

clear spantree portpri

Resets the configuration to the default value for the priority of a network port or ports for selection as part of the path to the STP root bridge in all VLANs on an MX.

Syntax

- **set spantree portpri** on page 13-362
- **set spantree portvlanpri** on page 13-363
- **show spantree** on page 13-364

clear spantree statistics

Clears STP statistics counters for a network port or ports and resets them to 0.

Syntax **clear spantree statistics** *port-list* [**vlan** *vlan-id*]

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command clears STP statistics counters for ports 5, 11, and 19 through 22, for all VLANs:

```
MX# clear spantree statistics 5,11,19-22
success: change accepted.
```

See Also **show spantree statistics** on page 13-369

set spantree

See Also **show spantree** on page 13-364

set spantree backbonefast

Enables or disables STP backbone fast convergence on an MX. This feature accelerates port recovery following the failure of an indirect link.

Syntax **set spantree backbonefast** {**enable** | **disable**}

enable	Enables backbone fast convergence.
disable	Disables backbone fast convergence.

Defaults STP backbone fast path convergence is disabled by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

Examples The following command enables backbone fast convergence:

```
MX# set spantree backbonefast enable
success: change accepted.
```

See Also **show spantree backbonefast** on page 13-366

set spantree fwddelay

Changes the period of time after a topology change that an MX which is not the root bridge waits to begin forwarding Layer 2 traffic on one or all of the configured VLANs. (The root bridge always forwards traffic.)

Syntax **set spantree fwddelay** *delay* {**all** | **vlan** *vlan-id*}

delay	Delay value. You can specify from 4 through 30 seconds.
all	Changes the forwarding delay on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the forwarding delay on only the specified VLAN.

Defaults The default forwarding delay is 15 seconds.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command changes the forwarding delay on VLAN to 20 seconds:

```
MX# set spantree fwddelay 20 vlan pink
success: change accepted.
```

See Also **show spantree** on page 13-364

set spantree hello

Changes the interval between STP hello messages sent by an MX when operating as the root bridge, on one or all of the configured VLANs.

Syntax **set spantree hello** *interval* {**all** | **vlan** *vlan-id*}

interval	Interval value. You can specify from 1 through 10 seconds.
all	Changes the interval on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the interval on only the specified VLAN.

Defaults The default hello timer interval is 2 seconds.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command changes the hello interval for all VLANs to 4 seconds:

```
MX# set spantree hello 4 all
success: change accepted.
```

See Also **show spantree** on page 13-364

set spantree maxage

Changes the maximum age for an STP root bridge hello packet that is acceptable to an MX acting as a designated bridge on one or all of its VLANs. After waiting this period of time for a new hello packet, the MX determines that the root bridge is unavailable and issues a topology change message.

Syntax **set spantree maxage** *aging-time* {**all** | **vlan** *vlan-id*}

aging-time	Maximum age value. You can specify from 6 through 40 seconds.
all	Changes the maximum age on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the maximum age on only the specified VLAN.

Defaults The default maximum age for root bridge hello packets is 20 seconds.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command changes the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds:

```
MX# set spantree maxage 15 all
success: change accepted.
```

See Also **show spantree** on page 13-364

set spantree portcost

Changes the cost that transmission through a network port or ports in the default VLAN on an MX adds to the total cost of a path to the STP root bridge.

Syntax **set spantree portcost** *port-list* **cost** *cost*

port-list	List of ports. MSS applies the cost change to all the specified ports.
cost *cost*	Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.

Defaults The default port cost depends on the port speed and link type. **Table 1** lists the defaults for STP port path cost.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage This command applies only to the default VLAN (VLAN 1). To change the cost of a port in another VLAN, use the **(33)**

See Also **show spantree portfast** on page 13-367

set spantree portpri

Changes the STP priority of a network port or ports for selection as part of the path to the STP root bridge in the default VLAN on an MX.

Syntax **set spantree portpri** *port-list* **priority** *value*

Defaults The default STP priority for all network ports is 128.

Access Enable command

History Introduced in MSS Version 1.0.

Usage This command applies only to the default VLAN (VLAN 1). To change the priority of a port in another VLAN, use the **set spantree portvlanpri** command.

Examples The following command sets the priority of ports 3 and 4 to 48:

```
MX# set spantree port-6( 9 2p9.96t.the pt.th4 6(eeria 9 2p)6t.the48 1 Tf-21.1446 -1.[(e)002846( sp)cd )6]
```

See Also

- **clear spantree portcost** on page 13-355
- **clear spantree portvlancost** on page 13-357
- **set spantree portcost** on page 13-360
- **show spantree** on page 13-364
- **show spantree portvlancost** on page 13-368

set spantree portvlanpri

Examples The following command sets the bridge priority of VLAN to 69:

```
MX# set spantree priority 69 vlan pink
success: change accepted.
```

See Also **show spantree** on page 13-364

set spantree uplinkfast

Enables or disables STP uplink fast convergence on an MX. This feature enables an MX with redundant links to the network backbone to immediately switch to the backup link to the root bridge if the primary link fails.

Syntax **set spantree uplinkfast** {**enable** | **disable**}

Defaults Disabled.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage The uplink fast convergence feature is applicable to bridges acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on MX switches that are in the network core.

Examples The following command enables uplink fast convergence:

```
MX# set spantree uplinkfast enable
success: change accepted.
```

See Also **show spantree** on page 13-364

Examples The following command displays STP information for VLAN :

```
MX# show spantree vlan default
VLAN     1
Spanning Tree Mode           PVST+
Spanning Tree Type           IEEE
Spanning Tree Enabled

Designated Root              00-02-4a-70-49-f7
Designated Root Priority     32768
Designated Root Path Cost    19
Designated Root Port         1
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-02-76-f7
Bridge ID Priority           32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port               Vlan      STP-State     Cost   Prio    Portfast
-------------------------------------------------------------------------------
1                    1       Forwarding      19   128     Disabled
2                    1       STP Off         19   128     Disabled
3                    1       Disabled        19   128     Disabled
4                    1       Disabled        19   128     Disabled
5                    1       Disabled        19   128     Disabled
6                    1       Disabled        19   128     Disabled
7                    1       Disabled        19   128     Disabled
8                    1       Disabled        19   128     Disabled
```

Table 13– 1 describes the fields in this display.

VLAN	VLAN number.
Spanning Tree Mode	In the current software version, the mode is always , which means Per VLAN Spanning Tree+.
Spanning Tree Type	In the current software version, the type is always , which means STP is based on the IEEE 802 standards.
Spanning Tree Enabled	State of STP on the VLAN.
Designated Root	MAC address of the spanning tree root bridge.
Designated Root Priority	Bridge priority of the root bridge.
Designated Root Path Cost	Cumulative cost from this bridge to the root bridge. If this MX is the root bridge, then the root cost is 0.
Designated Root Port	Port through which this MX reaches the root bridge. If this MX switch is the root bridge, this field says .
Root Max Age	Maximum acceptable age for hello packets on the root bridge.
Root Hello Time	Hello interval on the root bridge.
Root Forward Delay	Forwarding delay value on the root bridge.
Bridge ID MAC ADDR	The MX MAC address.
Bridge ID Priority	The MX bridge priority.
Bridge Max Age	The MX maximum acceptable age for hello packets.
Bridge Hello Time	The MX hello interval.
Bridge Forward Delay	The MX forwarding delay value.

See Also **set spantree backbonefast** on page 13-359

show spantree blockedports

Lists information about MX ports that STP has blocked on one or all of the VLANs.

Syntax **show spantree blockedports** [**vlan** *vlan-id*]

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays information for blocked ports on all VLANs.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Usage The command lists information separately for each VLAN.

Examples The following command shows information about blocked ports on an MX for the VLAN (VLAN 1):

```
MX# show spantree blockedports vlan default

Port               Vlan       Port-State    Cost   Prio   Portfast
-------------------------------------------------------------------------
22                  190        Blocking         4   128     Disabled

Number of blocked ports (segments) in VLAN 1 : 1
```

The port information is the same as the information displayed by the **show spantree** command. See Table 13– 1 on page 365.

See Also **show spantree** on page 13-364

show spantree portfast

Displays STP uplink fast convergence information for all network ports or for one or more network ports.

Syntax **show spantree portfast** [*port-list*]

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command shows uplink fast convergence information for all ports:

```
MX# show spantree portfast
Port                       Vlan   Portfast
-------------------------- ----   ----------
1                          1      disable
2                          1      disable
3                          1      disable
4                          1      enable
5                          1      disable
```

```
6                               1       disable
7                               1       disable
8                               1       disable
10                              1       disable
15                              1       disable
16                              1       disable
17                              1       disable
18                              1       disable
19                              1       disable
20                              1       disable
21                              1       disable
22                              1       disable
11                              2       enable
12                              2       disable
13                              2       disable
14                              2       enable
```

Table 13– 2 describes the fields in this display.

Port	Port number.
VLAN	VLAN number.
Portfast	State of the uplink fast convergence feature: ❑ Enable ❑ Disable

See Also **set spantree portfast** on page 13-361

show spantree portvlancost

Displays the cost of a port on a path to the STP root bridge, for each of the port of the VLANs.

Syntax **show spantree portvlancost** *port-list*

port-list List of ports.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command shows the STP port cost of port 1:

```
MX# show spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

See Also

- **clear spantree portcost** on page 13-355
- **clear spantree portvlancost** on page 13-357
- **set spantree portcost** on page 13-360
- **set spantree portvlancost** on page 13-362
- **show spantree** on page 13-364

show spantree statistics

Displays STP statistics for one or more MX network ports.

Syntax **show spantree statistics** [*port-list* [**vlan** *vlan-id*]]

Defaults None.

3Defaults(cs)T6 1 Tf98 0 0 98 T4.1 566.34 Tc40035 Tc0 AllNone.

```
message age timer                       ACTIVE
message age timer value                 0
topology change timer                   INACTIVE
topology change timer value             0
hold timer                              INACTIVE
hold timer value                        0
delay root port timer                   INACTIVE
delay root port timer value             0
delay root port timer restarted is      FALSE


            VLAN based information & statistics

spanning tree type                      ieee
spanning tree multicast address         01-00-0c-cc-cc-cd
bridge priority                         32768
bridge MAC address                      00-0b-0e-12-34-56
bridge hello time                       2
bridge forward delay                    15
topology change initiator:              0
last topology change occured:           Tue Jul 01 2003 22:33:36.
topology change                         FALSE
topology change time                    35
topology change detected                FALSE
topology change count                   1
topology change last recvd. from        00-0b-0e-02-76-f6


            Other port specific info

dynamic max age transition              0
port BPDU ok count                      21825
msg age expiry count                    0
link loading                            0
BPDU in processing                      FALSE
num of similar BPDU's to process        0
received_inferior_bpdu                  FALSE
next state                              0
src MAC count                           21807
total src MAC count                     21825
curr_src_mac                            00-0b-0e-00-04-30
next_src_mac                            00-0b-0e-02-76-f6
```

Table 13– 3 describes the fields in this display.

Port	Port number.
VLAN	VLAN ID.
Spanning Tree enabled for vlan	State of the STP feature on the VLAN.
port spanning tree	State of the STP feature on the port.

state	STP state of the port: ❑ Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. ❑ Disabled—The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected. ❑ Forwarding—The port is forwarding Layer 2 traffic. ❑ Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding. ❑ Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.
port_id	STP port ID.
port_number	STP port number.
path cost	Cost to use this port to reach the root bridge. This is part of the total path cost (designated cost).
message age	Age of the protocol information for a port and the value of the maximum age parameter (shown in parenthesis) recorded by the switch.
designated_root	MAC address of the root bridge.
designated cost	Total path cost to reach the root bridge.
designated_bridge	Bridge to which this MX forwards traffic away from the root bridge.
designated_port	STP port through which this MX forwards traffic away from the root bridge.
top_change_ack	Value of the topology change acknowledgment flag in the next configured bridge protocol data unit (BPDU) to be transmitted on the associated port. The flag is set in reply to a topology change notification BPDU.
config_pending	Indicates whether a configured BPDU is to be transmitted on expiration of the hold timer for the port.

message age timer	Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.
message age timer value	Current value of the message age timer, in seconds.
topology change timer	Status of the topology change timer. This timer determines the time period during which configured BPDUs are transmitted with the topology change flag set by this MX switch when it is the root bridge, after detection of a topology change.
topology change timer value	Current value of the topology change timer, in seconds.
hold timer	Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.
hold timer value	Current value of the hold timer, in seconds.
delay root port timer	Status of the delay root port timer, which enables fast convergence when uplink fast convergence is enabled.
delay root port timer value	Current value of the delay root port timer.
delay root port timer restarted is	Whether the delay root port timer has been restarted.
spanning tree type	Type of spanning tree. The type is always IEEE.
spanning tree multicast address	Destination address used to send out configured BPDUs on a bridge port.
bridge priority	STP priority of this MX.
bridge MAC address	MAC address of this MX switch.
bridge hello time	Value of the hello timer interval, in seconds, when this MX switch is the root or is attempting to become the root.
bridge forward delay	Value of the forwarding delay interval, in seconds, when this MX switch is the root or is attempting to become the root.
topology change initiator	Port number that initiated the most recent topology change.
last topology change occurred	System time when the most recent topology change occurred.
topology change	Value of the topology change flag in configuration BPDUs to be transmitted by this MX switch on VLANs for which the switch is the des 0 (t)(y)5.na initiator0003 Tw[(n)6.R8(e)-1(s.)-4...na initiaddress of t75(g)-4.3(e)-1.4(

See Also **clear spantree statistics** on page 13-358

show spantree uplinkfast

Displays uplink fast convergence information for one VLAN or all VLANs.

Syntax **show spantree uplinkfast** [**vlan** *vlan-id*]

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command shows uplink fast convergence information for all VLANs:

```
MX# show spantree uplinkfast
 VLAN    port    list
------------------------------------------------------------------------
1       1(fwd),2,3
```

Table 13– 4 describes the fields in this display.

See Also **set spantree uplinkfast** on page 13-364

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on an MX. This chapter presents IGMP snooping commands alphabetically. Use the following table to locate commands in this chapter based on their use.

clear igmp statistics

Clears IGMP statistics counters on one VLAN or all VLANs on an MX and resets them to 0.

Syntax **clear igmp statistics** [**vlan** *vlan-id*]

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command clears IGMP statistics for all VLANs:

```
MX# clear igmp statistics
IGMP statistics cleared for all vlans
```

set igmp mrouter

Adds or removes a port in an MX list of ports that the MX forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

Syntax **set igmp mrouter port** *port-list* {**enable** | **disable**}

port *port-list*	Port list. MSS adds or removes the specified ports in the list of static multicast router ports.
enable	Adds the port to the list of static multicast router ports.
disable	Removes the port from the list of static multicast router ports.

Defaults By default, no ports are static multicast router ports.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You cannot add MP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples The following command adds port 9 as a static multicast router port:

```
MX# set igmp mrouter port 9 enable
success: change accepted.
```

The following command removes port 9 from the static multicast router port list:

```
MX# set igmp mrouter port 9 disable
success: change accepted.
```

See Also **show igmp mrouter** on page 14-385

set igmp mrsol

Enables or disables multicast router solicitation by an MX switch on one VLAN or all VLANs.

Syntax **set igmp mrsol** {**enable** | **disable**} [**vlan** *vlan-id*]

enable	Enables multicast router solicitation.
disable	Disables multicast router solicitation.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs.

Defaults Multicast router solicitation is disabled on all VLANs by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command enables multicast router solicitation on VLAN :

```
MX# set igmp mrsol enable vlan orange
success: change accepted.
```

See Also **set igmp mrsol mrsi** on page 14-378

set igmp mrsol mrsi

Changes the interval between multicast router solicitations by an MX on one VLAN or all VLANs.

Syntax **set igmp mrsol mrsi** *seconds* [**vlan** *vlan-id*]

seconds	Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS changes the multicast router solicitation interval for all VLANs.

Defaults The interval between multicast router solicitations is 30 seconds by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following example changes the multicast router solicitation interval to 60 seconds:

```
MX# set igmp mrsol mrsi 60
success: change accepted.
```

See Also **set igmp mrsol** on page 14-377

set igmp oqi

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on an MX switch.

Syntax **set igmp oqi** *seconds* [**vlan** *vlan-id*]

oqi *seconds*	Number of seconds that the MX waits for a general query to arrive before becoming the querier. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults The default other-querier-present interval is 255 seconds (4.25 minutes).

Access Enabled.

History Introduced in MSS Version 1.0.

Usage An MX cannot become the querier unless the pseudo-querier feature is enabled on the switch. When the feature is enabled, the switch becomes the querier for a subnet so long as the switch does not receive a query message from a router with a lower IP address than the IP address of the switch in that subnet. To enable the pseudo-querier feature, use **set igmp querier**.

Examples The following command changes the other-querier-present interval on VLAN to 200 seconds:

```
MX# set igmp oqi 200 vlan orange
success: change accepted.
```

See Also

- **set igmp lmqi** on page 14-376
- **set igmp qi** on page 14-379
- **set igmp qri** on page 14-380

- **set igmp querier** on page 14-380
- **set igmp mrouter** on page 14-377
- **set igmp rv** on page 14-381

set igmp proxy-report

Disables or reenables proxy reporting by an MX switch on one VLAN or all VLANs.

Syntax **set igmp proxy-report** {**enable** | **disable**} [**vlan** *vlan-id*]

Defaults Proxy reporting is enabled on all VLANs by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the MX sends all membership reports to the routers, including multiple reports for the same group.

Examples The following example disables proxy reporting on VLAN :

```
MX# set igmp proxy-report disable vlan orange
success: change accepted.
```

See Also

See Also

- **set igmp lmqi** on page 14-376
- **set igmp oqi** on page 14-378
- **set igmp qri** on page 14-380
- **set igmp querier** on page 14-380
- **set igmp mrouter** on page 14-377
- **set igmp rv** on page 14-381

set igmp qri

disable	Disables the pseudo-querier.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

Defaults The pseudo-querier is disabled on all VLANs by default.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Trapeze Networks recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

Examples The following example enables the pseudo-querier on the VLAN:

```
MX# set igmp querier enable vlan orange
success: change accepted.
```

See Also **show igmp querier** on page 14-386

set igmp receiver

Adds or removes a network port in the list of ports on which an MX switch forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

Syntax **set igmp receiver port** *port-list* {**enable** | **disable**}

port *port-list*	Network port list. MSS adds the specified ports to the list of static multicast receiver ports.
enable	Adds the port to the list of static multicast receiver ports.
disable	Removes the port from the list of static multicast receiver ports.

Defaults By default, no ports are static multicast receiver ports.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage You cannot add MP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples The following command adds port 7 as a static multicast receiver port:

```
MX# set igmp receiver port 7 enable
success: change accepted.
```

The following command removes port 7 from the list of static multicast receiver ports:

```
MX# set igmp receiver port 7 disable
success: change accepted.
```

See Also **show igmp receiver-table** on page 14-387

set igmp rv

Changes the robustness value for one VLAN or all VLANs on an MX switch. Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

```
router information:
Port Mrouter-IPaddr Mrouter-MAC        Type  TTL
---- -------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    17
Group           Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none              none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   258
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   258
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   258
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   258
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   258
Querier information:
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
IGMP vlan member ports: 10, 12, 11, 14, 16, 15, 13, 18, 17, 1, 20, 21, 2,
22, 19, 4, 6, 5, 3, 8, 7, 9
IGMP static ports: none
IGMP statistics for vlan orange:


IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries          0           0       0
GS-Queries               0           0       0
Report V1                0           0       0
Report V2                5           1       4
Leave                    0           0       0
Mrouter-Adv              0           0       0
Mrouter-Term             0           0       0
Mrouter-Sol             50         101       0
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
Topology notifications: 0
Packets with.lnIGMPtTyp: 50
Packets withbaedlGegit: 50
Packets withbaedic: 0
PacketsdDropped:4
```

Configuration values (lmqi)	Last member query interval.
Configuration values (rvalue)	Robustness value.
Multicast router information	List of multicast routers and active multicast groups. The fields containing this information are described separately. The **show igmp mrouter** command shows the same information.
Port	Number of the physical port through which the MX switch can reach the router.
Mrouter-IPaddr	IP address of the multicast router interface.
Mrouter-MAC	MAC address of the multicast router interface.
Type	How the MX learned that the port is a multicast router port: ❑

See Also

- **show igmp mrouter** on page 14-385
- **show igmp querier** on page 14-386
- **show igmp receiver-table** on page 14-387
- **show igmp statistics** on page 14-388

show igmp mrouter

Displays the multicast routers in an MX subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the switch can reach the router.

Syntax **show igmp mrouter** [**vlan** *vlan-id*]

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays the multicast routers in all VLANs.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command displays the multicast routers in VLAN :

```
MX# show igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPaddr  Mrouter-MAC       Type  TTL
---- --------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    33
```

Table 14– 2 describes the fields in this display.

Multicast routers for vlan	VLAN containing the multicast routers. Ports are listed separately for each VLAN.
Port	Number of the physical port through which the MX can reach the router.
Mrouter-IPaddr	IP address of the multicast router.
Mrouter-MAC	MAC address of the multicast router.
Type	How the MX learned that the port is a multicast router port: ❑ conf — Static multicast port configured by an administrator ❑ madv—Multicast advertisement ❑ quer—IGMP query ❑ dvmrp—Distance Vector Multicast Routing Protocol (DVMRP) ❑ pimv1—Protocol Independent Multicast (PIM) version 1 ❑ pimv2—PIM version 2
TTL	Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is . Static multicast router entries do not age out.

See Also

- **set igmp mrouter** on page 14-377
- **show igmp mrouter** on page 14-385

show igmp querier

Displays information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

Syntax **show igmp querier** [**vlan** *vlan-id*]

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays querier information for all VLANs.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following command displays querier information for VLAN :

```
MX# show igmp querier vlan orange
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
```

The following command shows the information MSS displays when the querier is the MX:

```
MX# show igmp querier vlan default
Querier for vlan default:
I am the querier for vlan default, time to next query is 20
```

The output indicates how many seconds remain before the pseudo-querier on the switch broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

```
MX# show igmp querier vlan red
Querier for vlan red:
There is no querier present on vlan red
```

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.

Table 14– 3 on page 386 describes the fields in the display when a querier other than the MX switch is present.

Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier interface.
Querier-MAC	MAC address of the querier interface.
TTL	Number of seconds before this entry ages out if the MX switch does not receive a query message from the querier.

See Also **set igmp querier** on page 14-380

show igmp receiver-table

Displays the receivers to which an MX forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

Syntax **show igmp receiver-table** [**vlan** *vlan-id*] [**group** *group-ip-addr/mask-length*]

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays the multicast receivers on all VLANs.
group *group-ip-addr/mask-length*	IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, MSS displays the multicast receivers for all groups.

Defaults None.

Access All.

History Introduced in MSS Version 1.0.

Examples The following command displays all multicast receivers in VLAN :

```
MX# show igmp receiver-table vlan orange
VLAN: orange
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none              none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   179
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   179
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   179
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   179
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   179
```

The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
MX# show igmp receiver-table group 237.255.255.0/24
VLAN: red
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
237.255.255.2      2     10.10.20.19 00:02:04:06:09:0d   112
237.255.255.119    3     10.10.30.31 00:02:04:06:01:0b   112

VLAN: green
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
237.255.255.17    11     10.10.40.41 00:02:06:08:02:0c    12
237.255.255.255    6     10.10.60.61 00:05:09:0c:0a:01   111
```

Table 14– 4 describes the fields in this display.

VLAN	VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN.
Session	IP address of the multicast group being received.
Port	Physical port through which the MX switch can reach the receiver.
Receiver-IP	IP address of the receiver.

See Also **set igmp receiver** on page 14-381

See Also **clear igmp statistics** on page 14-375

Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering.

(Security ACLs are different from the location policy on an MX, which helps you locally control user access. For location policy commands, see Chapter , “AAA Commands,” on page 9-147.)

This chapter presents security ACL commands alphabetically. Use the following table to locate commands in this chapter based on their use.

clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command **commit security acl**, clears the ACE from the running configuration.

Syntax **clear security acl** {*acl-name* | **all**} [*editbuffer-index*]

Defaults None.

Access Enabled.

History

Usage This command deletes security ACLs only in the edit buffer. You must use the **commit security acl** command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The **clear security acl** command deletes a security ACL, but does not stop the current filtering function if the ACL is mapped to any virilteede9Ns (.0038V.irua-2(.0038)4(edpp)4oCys,L or if the ACL

clear security acl map

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on an MX .

Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local MX database, use the command **clear user attr**, **clear mac-user attr**, **clear usergroup attr**, or **clear mac-usergroup attr**. To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.

Syntax **clear security acl map** {*acl-name* | **all**} {**vlan** *vlan-id* | **port** *port-list* [**tag** *tag-value*] | **ap** *apnum*} {**in** | **out**}

acl-name	Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
all	Removes security ACL mapping from all physical ports, virtual ports, and VLANs on an MX switch.
vlan *vlan-id*	VLAN name or number. MSS removes the security ACL from the specified VLAN.
port *port-list*	Port list. MSS removes the security ACL from the specified MX physical port or ports.
tag *tag-value*	Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4095. MSS removes the security ACL from the specified virtual port.
ap *apnum*	One or more MPs, based on

Defaults None.

Access Enabled.

History

Usage To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or Distributed MP and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

Examples To clear the mapping of security ACL from port 4 for incoming packets, type the following command:

```
MX# clear security acl map acljoe port 4 in
clear mapping accepted
```

To clear all physical ports, virtual ports, and VLANs of mapped ACLs on an MX for incoming and outgoing traffic, type the following command:

```
MX# clear security acl map all
```

```
success: change accepted.
```

See Also

- **clear security acl** on page 15-391
- **set security acl map** on page 15-400
- **show security acl map** on page 15-405

commit security acl

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the MX. Or, when used with the **clear security acl** command, **commit security acl** deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

Syntax **commit security acl** {*acl-name* | **all**}

acl-name	Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.
all	Commits all security ACLs in the edit buffer.

Defaults None.

Access Enabled.

History

MSS Version 1.0	Command introduced.
MSS Version 1.1	ACL names changed from case-sensitive to case-insensitive.

Usage Use the **commit security acl** command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single **commit security acl all** command commits the creation and/or deletion of whatever **show security acl info all editbuffer** shows to be currently stored in the edit buffer.

Examples The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
MX# commit security acl all
configuration accepted

MX# show security acl
ACL table

ACL                     Type  Class   Mapping
----------------------  ----  ------  -------
acl_123                 IP    Static
acl_124                 IP    Static

MX# show security acl info all editbuffer
acl editbuffer information for all
```

See Also

- **clear security acl** on page 15-391
- **rollback security acl** on page 15-395

- **set security acl** on page 15-395
- **show security acl** on page 15-402
- **show security acl info** on page 15-404

hit-sample-rate

This command has been renamed in MSS Version 4.1. To configure the hit sample rate, see **set security acl hit-sample-rate** on page 15-401.

rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

Syntax **rollback security acl** {*acl-name* | **all**}

acl-name	Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.
all	Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

Defaults None.

Access Enabled.

History

MSS Version 1.0	Command introduced.
MSS Version 1.1	ACL names changed from case-sensitive to case-insensitive.

Examples The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to security , and show the edit buffer after the rollback:

```
MX# show security acl info all editbuffer
ACL edit-buffer information for all

set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)
---------------------------------------------------------
1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits

MX# rollback security acl acl_122

MX# show security acl info all editbuffer
ACL edit-buffer information for all
```

See Also **show security acl** on page 15-402

set security acl

In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, UDP, MAC address packet information.

Syntax

By source address

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} {*source-ip-addr mask* | **any**} [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By Layer 4 protocol

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} *protocol-number* {*source-ip-addr mask* | **any**} {*destination-ip-addr mask* | **any**} [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *codepoint*]] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By IP packets

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **ip** {*source-ip-addr mask* | **any**} {*destination-ip-addr mask* | **any**} [[**precedence** *precedence*] [**tos** *tos*

acl-name	Security ACL name. ACL names must be unique within the MX, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters: ❑ Letters through and through ❑ Numbers 0 through 9 ❑ Hyphen (-), underscore (_), and period (.)

Defaults By default, permitted packets are classified based on DSCP value, which is converted

set security acl map

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or Distributed MP on the MX switch.

Syntax **set security acl map** *acl-name* {**vlan** *vlan-id* | **port** *port-list* [**tag** *tag-list*] | **ap** *apnum*} {**in** | **out**}

Defaults None.

Access Enabled.

History

- **set mac-user attr** on page 9-177
- **set mac-usergroup attr** on page 9-182
- **set security acl** on page 15-395
- **set user attr** on page 9-185
-

```
--------------------------- ---- -------------
acl_111                     IP   Not committed
acl-a                       IP   Not committed
```

To view details about these uncommitted ACLs, type the following command.

```
MX# show security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl-111 (ACEs 3, add 3, del 0, modified 2)
--------------------------------------------------
 1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP any
 3. deny SRC source IP 192.168.253.1 0.0.0.255
set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
--------------------------------------------------
 1. permit SRC source IP 192.168.1.1 0.0.0.0
```

See Also

- **clear security acl** on page 15-391
- **commit security acl** on page 15-394
- **set security acl** on page 15-395
- **show security acl** on page 15-402
- **show security acl info** on page 15-404

show security acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the MX. Each time a packet is filtered by a security ACL, the hit counter increments.

Syntax **show security acl hits**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage For MSS to count hits for a security ACL, you must specify **hits** in the **set security acl** commands that define ACE rules for the ACL.

Examples To display the security ACL hits on an MX, type the following command:

```
MX# show security acl hits
ACL hit-counters

Index Counter              ACL-name
----- -------------------- --------
    1                    0 acl_2
    2                    0 acl_175
    3                  916 acl_123
```

See Also

- **hit-sample-rate** on page 15-395
- **set security acl** on page 15-395

show security acl info

Displays the contents of a specified security ACL or all security ACLs that are committed—saved in the running configuration and nonvolatile storage—or the contents of security ACLs in the edit buffer before they are committed.

Syntax **show security acl info** [*acl-name* | **all**] [**editbuffer**]

acl-name	Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive.
all	Displays the contents of all security ACLs.
editbuffer	Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with **set security acl**. If you do not use

Defaults None.

Access Enabled.

History

Examples To display the contents of all security ACLs committed on an MX, type the following command:

```
MX# show security acl info
ACL information for all

set security acl ip acl_123 (hits #5 462)
----------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any

set security acl ip acl_134 (hits #3 0)
----------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits

set security acl ip acl_135 (hits #2 0)
----------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

The following command displays the contents of in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

```
MX# show security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123

set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
----------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
```

See Also

- **clear security acl** on page 15-391
- **commit security acl** on page 15-394

- **set security acl** on page 15-395

show security acl map

Displays the VLANs, ports, and virtual ports on the MX that a security ACL is assigned.

Syntax **show security acl map** *acl-name*

acl-name	Name of an existing security ACL to display static mapping. ACL names must start with a letter and are case-insensitive.

Defaults None.

Access Enabled.

History

MSS Version 1.0	Command introduced
MSS Version 1.1	ACL names changed from case-sensitive to case-insensitive

Examples The following command displays the port to which security ACL is mapped:

```
MX# show security acl map acl_111
ACL acl_111 is mapped to:

Port 4 in
```

See Also

- **clear security acl map** on page 15-393
- **set security acl map** on page 15-400
- **show security acl** on page 15-402

show security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the MX.

Syntax **show security acl resource-usage**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage Use this command with the help of the Trapeze Technical Assistance Center (TAC) to diagnose an ACL resource problem. (To contact TAC, see **"Contacting the Technical Assistance Center" on page 1–1**.)

Examples To display security ACL resource usage, type the following command:

```
MX# show security acl resource-usage
ACL resources

Classifier tree counters
------------------------
  Number of rules           : 2
  Number of leaf nodes      : 1
  Stored rule count         : 2
  Leaf chain count          : 1
```

```
Longest leaf chain        : 2
Number of non-leaf nodes  : 0
Uncompressed Rule Count   : 2
Maximum node depth        : 1
Sub-chain count           : 0
```

No VLAN or PORT mapping	Application of security ACLs to MX VLANs or ports on the MX switch: ❑ True—No security ACLs are mapped to VLANs or ports. ❑ False—Security ACLs are mapped to VLANs or ports.
No VPORT mapping	Application of security ACLs to MX virtual ports on the MX switch: ❑ True—No security ACLs are mapped to virtual ports. ❑ False—Security ACLs are mapped to virtual ports.

A digital certificate is a form of electronic identification for computers. The MX requires digital certificates to authenticate communications to RingMaster and Web View, to WebAAA clients, and to Extensible Authentication Protocol (EAP) clients for which the MX performs all EAP processing. Certificates can be generated on the MX or obtained from a certificate authority (CA). Keys contained within the certificates allow the MX, the servers, and the wireless clients to exchange information secured by encryption.

This chapter presents cryptography commands alphabetically. Use the following table to locate commands in this chapter based on their use.

crypto ca-certificate

Installs a certificate authority's own PKCS #7 certificate into the MX certificate and key storage area.

Syntax **crypto ca-certificate** {**admin** | **eap** | **web**} *PEM-formatted-certificate*

Defaults None.

Access Enabled.

History

Usage The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS #7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

To use this command, you must already have obtained a copy of the certificate from the certificate authority as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an AS

crypto certificate

Installs one of the MX PKCS #7 certificates into the certificate and key storage area on the MX. The certificate, which is issued and signed by a certificate authority, authenticates the MX either to RingMaster or Web View, or to 802.1X supplicants (clients).

Syntax

crypto generate key

Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, generates an authentication key.

Syntax **crypto generate key** {**admin** | **domain** | **eap** | **ssh** | **web**} {**128** | **512** | **1024** | **2048**}

Defaults None.

Access Enabled.

History

Usage You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow MSS to generate it automatically. The first time an SSH client attempts to access the SSH server on an MX, the MX automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

Examples To generate an administrative key for use with RingMaster, type the following command:

```
MX# crypto generate key admi y(e)6(ee)
```

State Name: **CA**
Locality Name: **Pleasanton**
Organizational Name: **Trapeze**
Organizational Unit: **ENG**
Common Name: **ENG**
Email Address: **admin@example.com**
Unstructured Name: **admin**
CSR for admin is

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQAwezELMAkGA1UEBhMCdXMxCzAJBgNVBAgTAmNhMQswCQYDVQQH
EwJjYTELMAkGA1UEChMCY2ExCzAJBgNVBAsTAmNhMQswCQYDVQQDEwJjYTEYMBYG
CSqGSIb3DQEJARYJY2FAY2EuY29tMREwDwYJKoZIhvcNAQkCEwJjYTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA1zatpYStOjHMa0QJmWHeZPPFGQ9kBEimJKPG
bznFjAC780GcZtnJPGqnMnOKj/4NdknonT6NdCd2fBdGbuEFGNMNgZMYKGcV2JIu
```

Name Common field is requ	Specify a un name for th MX. In numeric characters with no spaces. Use a fully qualified name if such your network supports. Maximum 30 name resolution is used on This

Note: If you are generating ab AAA (**web**) certificate, use a common name that looks like a domain name (wo or more strings connected by dots,

Defaults None.

Access Enabled.

Hist

Usage To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Exames To generate a self-signed administrative certificate, type the following command:

```
MX# crypto generate admin-cert for admin generated
```

See Also

- **crypto certificate** on page 16-411
- **crypto generate key** on page 16-412

crypto otp

Sets a one-time passw (OTP) for usith the **crypto pkc** command.

Syntax **crypto otp** {**admin** | **eap** | **web**} *one-time-password*

web Creates a one-time password for installing a PKCS #12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the MX to WebAAA clients.

one-time-password Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS #12 object file.

Note: On an MX providing communication to and from Microsoft Windows clients, use a one-time password of 31 characters or fewer.

The following characters be used as part of the one-time password of a PKCS #12 file:

- Quotation marks (“ ”)
- Question mark (?)
- Ampersand (&)

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 3.0	**webaaa** option added
Version 4.1	**webaaa** option renamed to **web**

Usage The password allows the public-private key pair and certificate to be installed together from the same PKCS #12 object file. MSS erases the one-time password after processing the **crypto pkcs12** command or when you reboot the MX.

Trapeze Networks recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

Examples The following command creates the one-time password for installing an EAP certificate and key pair:

```
MX# crypto generate otp eap hap9iN#ss
OTP set
```

See Also **crypto pkcs12** on page 16-416

crypto pkcs12

Unpacks a PKCS #12 object file into the certificate and key storage area on the MX. This object file contains a public-private key pair, an MX certificate signed by a certificate authority, and the certificate authority's certificate.

Syntax **crypto pkcs12** {**admin** | **eap** | **web**} *file-location-url*

admin Unpacks a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the MX to RingMaster or Web View.

eap Unpacks a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the MX to 802.1X supplicants (clients).

web	Unpacks a PKCS #12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the MX switch to WebAAA clients.
file-location-url	Location of the PKCS #12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces.

Defaults The password you enter with the **crypto otp** command must be the same as the one protecting the PKCS #12 file.

Access Enabled.

History

Version 1.0	Command -6(on6nc)-4.5(1 Tm)Tm.0027 Tc6.7(tsl)-6(48)oduc-6(48)ed( )-6(-loca)6.nto

Usage To use this command, you must have already created a one-time password with the **crypto otp** command.

You must also have the PKCS #12 object file available. You can download a PKCS #12 object file via TFTP from a remote location to the local nonvolatile storage system on the MX.

Examples The following commands copy a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's certificate—from a TFTP server to nonvolatile storage on the MX, create the one-time password , and unpack the PKCS #12 file:

```
MX# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

MX# crypto otp eap hap9iN#ss
OTP set

MX# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
```

See Also **crypto otp** on page 16-415

show crypto ca-certificate

Displays information about the certificate authority's PEM-encoded PKCS #7 certificate.

Syntax **show crypto ca-certificate** {**admin** | **eap** | **web**}

Defaults None.

Access Enabled.

History

Examples To display information about the certificate of a certificate authority, type the following command:

```
MX# show crypto ca-certificate
```

Table 16– 1 describes the fields in the display.

See Also

- **crypto ca-certificate** on page 16-410
- **show crypto certificate** on page 16-418

show crypto certificate

Displays information about one of the cryptographic certificates installed on the MX.

Syntax **show crypto certificate** {**admin** | **eap** | **web**}

Defaults **None.**

Examples To display information about a cryptographic certificate, type the following command:

```
MX# show crypto certificate eap
```

Table 16– 2 describes the fields of the display.

Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also

- **crypto generate self-signed** on page 16-414
- **show crypto ca-certificate** on page 16-417

show crypto key domain

Displays the checksum (also called a) of the public key used to authenticate management traffic between MX switches.

Syntax **show crypto key domain**

Defaults None.

Access Enabled.

History Introduced in MSS 5.0.

Examples To display the fingerprint for MX-MX security, type the following command:

```
MX# show crypto key domain
Domain public key:
e6:43:91:e2:b3:53:ed:46:76:5f:f0:96:3a:3b:86:d3
```

See Also **crypto generate key** on page 16-412

show crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a) of the public key. When you connect to the MX with an SSH client, you can compare the SSH key checksum displayed by the MX with the one displayed by the client to verify that you really are connected to the MX and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

Syntax **show crypto key ssh**

Defaults None.

Access Enabled.

History Introduced in MSS 2.0.

Examples To display SSH key information, type the following command:

```
MX# show crypto key ssh
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

See Also **crypto generate key** on page 16-412

clear radius

Defaults Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The MX does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

Access Enabled.

History Introduced in MSS 1.0.

Usage To override the globally set values on a particular RADIUS server, use the **set radius**

Usage The **clear radius client system-ip** command causes the MX to use the IP address of the interface through which the MX sends a RADIUS client request as the source IP address. The MX selects a source interface address based on information in the routing table as the source address for RADIUS packets leaving the MX.

Examples To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

```
MX# clear radius client system-ip
success: change accepted.
```

See Also

- **set radius client system-ip** on page 428
- **show aaa** on page 189

clear radius proxy client

Removes RADIUS proxy client entries for third-party APs.

Syntax **clear radius proxy client all**

Defaults None.

Access Enabled.

History Introduced in MSS 4.0.

Examples The following command clears all RADIUS proxy client entries from the switch:

```
MX# clear radius proxy client all
success: change accepted.
```

See Also **set radius proxy client** on page 429

clear radius proxy port

Removes RADIUS proxy ports configured for third-party APs.

Syntax **clear radius proxy port all**

Defaults None.

Access Enabled.

History Introduced in MSS 4.0.

Examples The following command clears all RADIUS proxy port entries from the switch:

```
MX# clear radius proxy port all
success: change accepted.
```

See Also **set radius proxy port** on page 429

clear radius server

Removes the named RADIUS server from the MX configuration.

Syntax **clear radius server** *server-name*

server-name Name of a RADIUS server configured to perform remote AAA services for the MX.

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Examples The following command removes the RADIUS server from a list of remote AAA servers:

```
MX# clear radius server rs42
success: change accepted.
```

See Also

- **set radius server** on page 430
- **show aaa** on page 189

clear server group

Removes a RADIUS server group from the configuration, or disables load balancing for the group.

Syntax **clear server group** *group-name* [**load-balance**]

group-name	Name of a RADIUS server group configured to perform remote AAA services for MX switches.
load-balance	Ability of group members to share demand for services among servers.

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Usage Deleting a server group removes the server group from the configuration. However, the members of the server group remain.

Examples To remove the server group type the following command:

```
MX# clear server group sg-77
success: change accepted.
```

To disable load balancing in a server group , type the following command:

```
MX# set server group shorebirds load-balance disable
success: change accepted.
```

See Also **set server group** on page 432

radping

Provides a diagnostic tool to enhance troubleshooting capabilities for RADIUS servers on the network. The command sends an authentication request to the RADIUS server to determine if it is offline.

Syntax MX# **radping** {**server** |*servername* | **group** *servergroup*}**request** [**acct-off** | **acct-on** | **acct-start** | **acct-stop** | **acct-update** | **authentication] user** *username* **password** *password* **auth-type** {**plain**|**mschap2**}

Defaults None

Access Enabled.

History Introduced in MSS Version 6.2.

Examples To verify that a RADIUS server, with the username, smith5, password, swordfish, is active on the network, type the following command:

```
MX# radping alpha request authentication user smith5 passassassassas4(;)6(fis)6( a)6(/TT)6(st)6e mschap
```

set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the MX automatically sets all these values except the password (key).

Syntax **set radius** {**author-password** *use-mac-address* | **deadtime** *minutes* | **das-port** *port* **encrypted-key** *string* | **key** *string* | [**mac-addr-format [colons | hyphens | one-hypen | raw]] retransmit** *number* | **timeout** *seconds*}

author-password *use-mac-address*	Set this option to send the user mac-address as the password.
das-port *port*	Set the dynamic authorization port for all DACs. The value can be 1, 65535, or 3799.
deadtime *minutes*	Number of minutes the MX waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes.
encrypted-key *string*	Password (shared secret key) used to authenticate to the RADIUS server, entered in its encrypted form. You must provide the same encrypted password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. MSS does not encrypt the string you enter, and instead displays the string in **show config** and **show aaa** output exactly as you entered it. **Note:** Use this option only if you are entering the key in the encrypted form. To enter the key in unencrypted form, use the **key** option instead.
key *string*	Password (shared secret key) used to authenticate to the RADIUS server, entered in its unencrypted form. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. MSS encrypts the displayed form of the string in **show config** and **show aaa** output. **Note:** Use this option only if you are entering the key in the unencrypted form. To enter the key in encrypted form, use the **encrypted-key** option instead.
mac-addr-format [colons | hyphens | one-hyphen | raw]	Sets the MAC address format for all RADIUS servers using the **author-password** option. MAC addresses can have the following formats: ❑ colons—12:34:56:78:9a:bc ❑ hyphens—12–34–56–78–9a–bc ❑ one-hyphen— 123456–789abc ❑ raw—123456789abc
retransmit *number*	Number of transmission attempts the MX makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
timeout *seconds*	Number of seconds the MX waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535.

Defaults Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The MX does not designate unresponsive RADIUS servers as unavailable.)
- **encrypted-key**—No key
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

Access Enabled.

History

Usage You can specify only one parameter per command line.

Examples The following commands sets the dead time to 5 minutes, the RADIUS key to , the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the MX switch:

```
MX-20# set radius deadtime 5
success: change accepted.

MX-20# set radius key goody
success: change accepted.

MX-20# set radius retransmit 1
success: change accepted.

MX-20# set radius timeout 21
success: change accepted.
```

See Also

- **clear radius server** on page 423
- **set radius server** on page 430
- **show aaa** on page 189

set radius client system-ip

Configure RADIUS to use the client system IP address as the source IP address for all RADIUS packets.

Syntax `set radius client system-ip`

Defaults None

Access Enabled

History Introduced in MSS Version 7.0

set radius dac

Configure dyanmic RADIUS extensions in support of RFC 3576.

Syntax `MX#set radius-dac` *name ip-addr* `key` *string* `[disconnect [enable|disable] change-of-author[enable|disable] replay-protection [enable|disable] replay-window` *seconds*`]`

Defaults None

Access Enabled.

set authorization dynamic

Configures SSIDs for dynamic RADIUS clients.

Syntax MX# **set authorization dynamic** {**ssid** [**wireless_8021X** |**8021X** |**any** |*name*] | **wired** *name*}

Defaults None.

Access Enabled.

History Introduced in MSS Version 6.2.

Examples To configure an SSID named dac_clients, use the following command:

```
MX# set authorization dynamic ssid dac_clients
success:change accepted.
```

set radius das-port

Configures the dynamic authorizatio

set radius proxy client

Adds a RADIUS proxy entry for a third-party AP. The proxy entry specifies the IP address of the AP and the UDP ports on which the MX listens for RADIUS traffic from the AP.

Syntax **set radius proxy client address** *ip-address* [**acct-port** *acct-udp-port-number*] [**port** *udp-port-number*] **key** *string*

address *ip-address*	IP address of the third-party AP. Enter the address in dotted decimal notation.
port *udp-port*	UDP port on which the MX listens for RADIUS access-requests from the AP.
acct-port *acct-udp-port*	UDP port on which the MX swtch listens for RADIUS stop-accounting records from the AP.
key *string*	Password (shared secret key) the MX uses to authenticate and encrypt RADIUS communication.

Defaults The default UDP port number for access-requests is 1812. The default UDP port number for stop-accounting records is 1813.

Access Enabled.

History Introduced in MSS 4.0.

Usage AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the .

Examples The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP ports 1812 and 1813 on the MX:

```
MX# set radius proxy client address 10.20.20.9 key radkey1
success: change accepted.
```

See Also

- **clear radius proxy client** on page 423
- **set authentication proxy** on page 172
- **set radius proxy port** on page 429

set radius proxy port

Configures the MX port connected to a third-party AP as a RADIUS proxy for the SSID supported by the AP.

Syntax **set radius proxy port** *port-list* [**tag** *tag-value*] **ssid** *ssid-name*

port *port-list*	MX port(s) connected to the third-party AP.
tag *tag-value*	802.1Q tag value in packets sent by the third-party AP for the SSID.
ssid *ssid-name*	SSID supported by the third-party AP.

Defaults None.

Access Enabled.

History Introduced in MSS 4.0.

Usage AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the .

Enter a separate command for each SSID, and the tag value that you want the MX to support.

Examples The following command maps SSID to packets received on port 3 or 4, using 802.1Q tag value 104:

```
MX# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

See Also

-

Defaults Default values are listed below:

- **auth-port**—UDP port 1812
- **acct-port**—UDP port 1813
- **timeout**—5 seconds
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **deadtime**—0 (zero) minutes (The MX does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **encrypted-key**—No key
- **author-password**—trapeze

Access Enabled.

History

Usage For a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be

set server group

Configures a group of one to four RADIUS servers.

Syntax **set server group** *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]

Defaults None.

Access Enabled.

History Introduced in MSS 1.0.

Usage You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.

Do not use the same name for a RADIUS server and a RADIUS server group.

Examples To set server group with members , , and , type the following command:

```
MX-20# set server group shorebirds members heron egret sandpiper
success: change accepted.
```

See Also

- **clear server group** on page 424
-

Examples To enable load balancing between the members of server group , type the following command:

```
MX-20# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between server group members, type the following command:

```
MX-20# set server group shorebirds load-balance disable
success: change accepted.
```

See Also

- **clear server group** on page 424
- **clear radius server** on page 423
- **set server group** on page 432
- **show aaa** on page 189

show radius

Displays configuration information about RADIUS servers.

Syntax

Use 802. IEEE X management commands to modify the default settings for IEEE 802.1X sessions on an MX. For best results, change the settings only if you are aware of a problem with 802.1X performance on the MX.

This chapter presents 802.1X commands alphabetically. Use the following table to locate commands in this chapter based on their use. For information about configuring 802.1X commands for user authentication, see

clear dot1x bonded-period

Resets the Bonded Auth period to its default value.

Syntax **clear dot1x max-req**

Defaults The default bonded authentication period is 0 seconds.

Access Enabled.

History Introduced in MSS Version 2.1.

Usage

Examples To reset the Bonded period to its default, type the following command:

```
MX# clear dot1x bonded-period
success: change accepted.
```

See Also

- **set dot1x bonded-period** on page 18-440
- **show dot1x** on page 18-446

clear dot1x max-req

Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the MX switch retransmits to a supplicant (client).

Syntax **clear dot1x max-req**

Defaults The default number is 20.

Access Enabled.

History Introduced in MSS 1.0.

Examples To reset the number of 802.1X requests the MX can send to the default setting, type the following command:

```
MX# clear dot1x max-req
success: change accepted.
```

See Also

- **set dot1x max-req** on page 18-441
- **show dot1x** on page 18-446

clear dot1x port-control

Resets all wired authentication ports on the MX to default 802.1X authentication.

Syntax **clear dot1x port-cp9p**

Usage Tisn

Examples Type the following command to reset the wired authentication port control:

```
MX# clear dot1x port-control
success: change accepted.
```

See Also

- **set dot1x port-control** on page 18-441
- **show dot1x** on page 18-446

clear dot1x quiet-period

Resets the quiet period after a failed authentication to the default setting.

Syntax **clear dot1x quiet-period**

Defaults The default is 60 seconds.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to reset the 802.1X quiet period to the default:

```
MX# clear dot1x quiet-period
success: change accepted.
```

See Also

- **set dot1x quiet-period** on page 18-442
- **show dot1x** on page 18-446

clear dot1x reauth-max

Resets the maximum number of reauthorization attempts to the default setting.

Syntax **clear dot1x reauth-max**

Defaults The default is 2 attempts.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to reset the maximum number of reauthorization attempts to the default:

```
MX# clear dot1x reauth-max
success: change accepted.
```

See Also

- **set dot1x reauth-max** on page 18-442
- **show dot1x** on page 18-446

clear dot1x reauth-period

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

Syntax **clear dot1x reauth-period**

Defaults The default is 3600 seconds (1 hour).

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to reset the default reauthentication time period:

```
MX# clear dot1x reauth-period
success: change accepted.
```

See Also

- **set dot1x reauth-period** on page 18-443
- **show dot1x** on page 18-446

clear dot1x timeout auth-server

Resets to the default setting the number of seconds that must elapse before the MX times out a request to a RADIUS server.

Syntax

set dot1x bonded-period

Changes the Bonded Auth™ (bonded authentication) period. The is the number of seconds MSS allows a Bonded Auth user to reauthenticate.

Syntax **set dot1x bonded-period** *seconds*

Defaults The default bonded period is 0 seconds, which disables the feature.

Access Enabled.

History Introduced in MSS 2.1.

Usage

set dot1x max-req

Sets the maximum number of times the MX retransmits an EAP request to a supplicant (client) before ending the authentication session.

Syntax **set dot1x max-req** *number-of-retransmissions*

Defaults The default number of EAP retransmissions is 2.

Access Enabled.

History Introduced in MSS 1.0.

Usage To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Examples Type the following command to set the maximum number of EAP request retransmissions to three attempts:

```
MX# set dot1x max-req 3
success: dot1x max request set to 3.
```

See Also

- **clear dot1x max-req** on page 18-436
- **v7.65.4()-6(ending the0et the)-.96 0 0 gf0n5 r**

- **show dot1x** on page 18-446

set dot1x quiet-period

Sets the number of seconds an MX remains quiet and does not respond to a supplicant after a failed authentication.

Syntax **set dot1x quiet-period** *seconds*

seconds	Specify a value between 0 and 65,535.

Defaults The default is 60 seconds.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to set the quiet period to 90 seconds:

```
MX# set dot1x quiet-period 90
success: dot1x quiet period set to 90.
```

See Also

- **clear dot1x quiet-period** on page 18-437
- **show dot1x** on page 18-446

set dot1x reauth

Determines whether the MX switch allows the reauthentication of supplicants (clients).

Syntax **set dot1x reauth** {**enable** | **disable**}

enable	Permits reauthentication.
disable	Denies reauthentication.

Defaults Reauthentication is enabled by default.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to enable reauthentication of supplicants (clients):

```
MX# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

See Also

- **set dot1x reauth-max** on page 18-442
- **set dot1x reauth-period** on page 18-443
- **show dot1x** on page 18-446

set dot1x reauth-max

Sets the number of reauthentication attempts that the MX makes before the supplicant (client) becomes unauthorized.

Syntax **set dot1x reauth-max** *number-of-attempts*

Defaults The default number of reauthentication attempts is 2.

Access Enabled.

History Introduced in MSS 1.0.

set dot1x timeout auth-server

Sets the number of seconds that must elapse before the MX switch times out a request to a RADIUS authentication server.

Syntax **set dot1x timeout auth-server** *seconds*

seconds	Specify a value between 1 and 65,535.

Defaults The default is 30 seconds.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to set the authentication server timeout to 60 seconds:

```
MX# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```

See Also

- **clear dot1x timeout auth-server** on page 18-438
- **show dot1x** on page 18-446

set dot1x timeout supplicant

Sets the number of seconds that must elapse before the MX switch times out an authentication session with a supplicant (client).

Syntax **set dot1x timeout supplicant** *seconds*

seconds	Specify a value between 1 and 65,535.

Defaults The default is 30 seconds.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to set the number of seconds for authentication session timeout to 300:

```
MX# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

See Also

- **clear dot1x timeout auth-server** on page 18-438
- **show dot1x** on page 18-446

set dot1x tx-period

Sets the number of seconds that must elapse before the MX switch retransmits an EAPoL packet.

Syntax **set dot1x tx-period** *seconds*

seconds	Specify a value between 1 and 65,535.

Defaults The default is 5 seconds.

Access Enabled.

History Introduced in MSS 1.0.

Examples Type the following command to set the number of seconds before the MX retransmits an EAPoL packet to 300:

```
MX# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

See Also

- **clear dot1x tx-period** on page 18-439
- **show dot1x** on page 18-446

set dot1x wep-rekey

Enables or disables Wired Equivalency Privacy (WEP) rekeying for broadcast and multicast encryption keys.

Syntax **set dot1X wep-rekey** {**enable** | **disable**}

enable	Causes the broadcast and multicast keys for WEP to be rotated at an interval set by the **set dot1x wep-rekey-period** for each radio, associated VLAN, and encryption type. The MX generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages.
disable	WEP broadcast and multicast keys are never rotated.

Defaults WEP key rotation is enabled, by default.

Access Enabled.

History Introduced in MSS 1.0.

Usage Reauthentication is required for WEP key rotation to take place. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio, VLAN, or encryption type receive the new keys at the same time.

Examples Type the following command to disable WEP key rotation:

```
MX# set dot1x wep-rekey disable
success: wep rekeying disabled
```

See Also

- **set dot1x wep-rekey-period** on page 18-445
- **show dot1x** on page 18-446

set dot1x wep-rekey-period

Sets the interval for rotating the WEP broadcast and multicast keys.

Syntax **set dot1x wep-rekey-period** *seconds*

seconds	Specify a value between 30 and 1,641,600 (19 days).

Defaults The default is 1800 seconds (30 minutes).

Access Enabled.

History

Examples Type the following command to set the WEP-rekey period to 300 seconds:

```
MX# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```

See Also

- **set dot1x wep-rekey** on page 18-445
- **show dot1x** on page 18-446

show dot1x

Displays 802.1X client information for statistics and configuration settings.

Syntax **show dot1x** {**clients** | **stats** | **config**}

Defaults None.

Access Enabled.

History

Examples Type the following command to display the 802.1X clients:

```
MX# show dot1x clients
```

```
00:05:5d:7e:94:89       Authenticated   vlan-eng        EXAMPLE\fmarshall
00:06:80:00:5c:02       Authenticated   vlan-eng        EXAMPLE\bmccarthy
00:02:2d:6a:de:f2       Authenticated   vlan-pm         neailey@xmple.com
00:02:2d:5e:5b:76       Authenticated   vlan-pm         EXAMPLE\tamara
00:02:2d:80:b6:e1       Authenticated   vlan-cs         dmc@xmple.com
00:30:65:16:8d:69       Authenticated   vlan-wep        MAC authenticated
00:02:2d:64:8e:1b       Authenticated   vlan-eng        EXAMPLE\wong
```

Type the following command to display the 802.1X configuration:

```
MX# show dot1x config

            802.1X user policy
          ----------------------
 'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
 'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)

        802.1X parameter                setting
        ----------------                -------
        supplicant timeout              30
        auth-server timeout             30
        quiet period                    5
        transmit period                 5
        reauthentication period         3600
        maximum requests                2
        key transmission                enabled
        reauthentication                enabled
        authentication control          enabled
        WEP rekey period                1800
        WEP rekey                       enabled
        Bonded period                   60

        port 5, authcontrol: auto, max-sessions: 16
        port 6, authcontrol: auto, max-sessions: 1
        port 7, authcontrol: auto, max-sessions: 1
        port 8, authcontrol: auto, max-sessions: 1
        port 9, authcontrol: auto, max-sessions: 1
        port 10, authcontrol: auto, max-sessions: 1
        port 11, authcontrol: auto, max-sessions: 1
        port 12, authcontrol: auto, max-sessions: 1
        port 13, authcontrol: auto, max-sessions: 1
        port 14, authcontrol: auto, max-sessions: 1
        port 15, authcontrol: auto, max-sessions: 1
        port 16, authcontrol: auto, max-sessions: 1
        port 22, authcontrol: auto, max-sessions: 16
```

Type the following command to display 802.1X statistics:

```
MX# show dot1x stats
        802.1X statistic                value
        ----------------                -----
        Enters Connecting:              709
        Logoffs While Connecting:       112
        Enters Authenticating:          467
        Success While Authenticating:   0
        Timeouts While Authenticating:  52
        Failures While Authenticating:  0
        Reauths While Authenticating:   0
        Starts While Authenticating:    31
        Logoffs While Authenticating:   0
        Starts While Authenticated:     85
```

```
        Logoffs While Authenticated:    1
        Bad Packets Received:           0
```

Table 18– 1 explains the counters in the **show dot1x stats** output.

Use session management commands to display and clear administrative and network user sessions. This chapter presents session management commands alphabetically. Use the following table to locate commands in this chapter based on their use.

clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

Syntax **clear sessions** {**admin** | **console** | **telnet** [**client** [*session-id*] | **mesh-ap** [**session-id** *session-id*]}

admin	Clears sessions for all users with administrative access to the MX through a Telnet or SSH connection or a console plugged into the switch.
console	Clears sessions for all users with administrative access to the MX through a console plugged into the switch.
telnet	Clears sessions for all users with administrative access to the MX through a Telnet connection.
telnet client [*session-id*]	Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID.
mesh-ap [*session-id*]	Clears all Mesh AP sessions, or clears an individual Mesh AP session identified by session ID.

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced.
Version 1.1	New option, **client** [ ], added to clear Telnet client sessions.
Version 6.0	New option, **mesh-ap**, added to clear Mesh AP sessions.

Examples To clear all administrator sessions type the following command:

```
MX# clear sessions admin
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```
MX# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative Telnet sessions, type the following command:

```
MX# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear Telnet client session 0, type the following command:

```
MX# clear sessions telnet client 0
```

See Also **show sessions** on page 19-451

clear sessions network

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

Syntax **clear sessions network** {**user** *user-glob* | **mac-addr** *mac-addr-glob* | **vlan** *vlan-glob* | **session-id** *local-session-id*}

user *user-glob*	Clears all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage The **clear sessions network** command clears network sessions by deauthenticating and, for wireless clients, disassociating them.

Examples To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

```
MX# clear sessions network mac-addr 00:01:02:03:04:05
```

To clear session 9, type the following command:

```
MX-20# clear sessions network session-id 9
SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d,
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)
```

To clear the session of user , type the following command:

```
MX-20# clear sessions network user Natasha
```

To clear the sessions of users whose name begins with the characters , type the following command:

```
MX-20# clear sessions network user Jo*
```

To clear the sessions of all users on VLAN , type the following command:

```
MX-20# clear sessions network vlan red
```

See Also

- **show sessions** on page 19-451
- **show sessions network** on page 19-453

show sessions

Displays session information and statistics for all users with administrative access to the MX, or for administrative users with either console or Telnet access.

Syntax **show sessions** [**admin** | **console** | **telnet** [**client**]]

admin	Displays sessions for all users with administrative access to the MX through a Telnet or SSH connection or a console plugged into the switch.
console	Displays sessions for all users with administrative access to the MX through a console plugged into the switch.
telnet	Displays sessions for all users with administrative access to the MX through a Telnet connection.
telnet client	Displays Telnet sessions from the CLI to remote devices.

Defaults None.

Access All, except for **show sessions telnet client**, which has enabled access.

History

Version 1.0	Command introduced.
Version 1.1	New option, **client**, added to display Telnet client sessions.
Version 2.0	New field added to list the type of administrative session.
Version 6.2	Added the ability to display all sessions

Examples To display information about all sessions, use the following command:

```
MX> show sessions

   User                 Sess        IP or MAC          VLAN      Port/
   Name                 ID          Address            Name      Radio
   --------------       ---------   --------------     ------
   engineering-05:0c:78 28*         10.7.255.2         yellow    5/1
   engineering-79:86:73 29*         10.7.254.3         red       2/1
   engineering-1a:68:78 30*         10.7.254.8         red       7/1
```

To view information about sessions of administrative users, type the following command:

```
MX> show sessions admin
Tty         Username              Time (s)    Type
-------     --------------------  --------    ----
tty0                              3644        Console
tty2        tech                  6           Telnet
tty3        sshadmin              381         SSH
```

Syntax **show sessions mesh-ap** [**session-id** *session-id* | **verbose**]

session-id *local-session-id*	Displays the specified Mesh AP session. To determine the local session ID for a Mesh AP session, use the **show sessions mesh-ap** command without the **session-id** option.
verbose	Provides detailed output for all Mesh AP sessions.

Defaults None.

Access All.

History Introduced in MSS Version 6.0.

Examples To view information about Mesh AP sessions, type the following command:

```
MX> show sessions mesh-ap

User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- ---------
00:0b:0e:17:bb:3f               2* 1.1.1.3           (none)        L    AP 2/2
```

Table 19– 3 describes the fields of **show sessions mesh-ap** output.

User Name	The MAC address of the authenticated Mesh AP.
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active.
IP or MAC Address	IP address of the Mesh AP.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Number of the port and radio through which the Mesh AP is accessing this session.

See Also **clear sessions** on page 19-449

show sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

Syntax **show sessions network** [**ap** *apnum* | **user** *user-glob* | **mac-addr** *mac-addr-glob* | **qos-profile** *profilename* | **ssid** *ssid-name* | **statistics** | **vlan** *vlan-glob* | **session-id** *session-id* | **wired**] [**verbose**]

ap apnum	Displays network sessions for a single MP.
user *user-glob*	Displays all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an sign (@) or a period (.). (For details, see **"User Globs" on page 2–7**.)

mac-addr *mac-addr-glob*	Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:). Or use the wildcard character (*) to specify a set of MAC addresses. (For details, see **"MAC Address Globs" on page 2–7**.)
qos-profile *profilename*	Displays all network sessions for a named QoS profile.
ssid *ssid-name*	Displays all network sessions for an SSID.
statistics	Displays network statistics.
vlan *vlan-glob*	Displays all network sessions on a single VLAN or a set of VLANs. Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an sign (@) or a period (.). (For details, see **"VLAN Globs" on page 2–8**.)
session-id *local-session-id*	Displays the specified network session. To find local session IDs, use the **show sessions** command. The **verbose** option is not available with this form of the **show sessions network** command.
wired	Displays all network sessions on wired authentication ports.
verbose	Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name.

Defaults None.

Access All.

History

Version 1.0	Command introduced.
Version 4.1	Output added to the **show network sessions verbose** command to indicate the user's authorization attributes and whether they were supplied through AAA or through configured SSID defaults in a service profile.
Version 4.2	❑ Host name field added to **show sessions network verbose** output. ❑ MP serial number added to **show sessions network verbose** output. ❑ The following fields added to **show sessions network session-id** output: • Local Id • SSID • Last Auth Time • Last Activity • Idle Time-To-Live • Login Type • Protocol • Session CAC ❑ Authentication Method field renamed to EAP Method.
Version 5.0	❑ New values for the source of user attribute values (attributes include Vlan-Name, Start-Date, and so on.) See Table 19– 5 on page 457.

Usage MSS displays information about network sessions in three types of displays. See the following tables for field descriptions.

Summary display	See Table 19– 4 on page 457.
Verbose display	See Table 19– 5 on page 457.
show sessions network session-id display	See Table 19– 6 on page 458.

The following command displays information about network session 88:

```
MX# show sessions network session-id 88
Name: Trapeze\jdoeh
Session Id:    88
Global Id:   SESS-88-00040f-876766-623fd6
Login Type: dot1x
SSID:        Rack-39-PM
IP Address:  10.2.39.217
MAC Address: 00:0f:66:f4:71:6d
AP/Radio:  10/1
State:       ACTIVE
Session Tag: 2
Host name: jdoeh-d410
Vlan Name:   default
Up time: 02:54:29

Roaming history:
Switch             AP/Radio         Association Time     Duration
---------          ---------        ---------------      --------

192.168.254.82   3/2              09/21/07 11:16:47  02:54:03


Session Start:   Wed Sep 20 21:19:27 2006 GMT
Last Auth Time:  Wed Apr 20 21:19:26 2006 GMT
Last Activity:   Wed Apr 20 21:19:49 2006 GMT  ( <15s ago)
Session Timeout: 0
Idle Time-To-Live: 175
EAP Method:      NONE, using server 172.16.0.1
Protocol: 802.11
CoS: flow-through
Session CAC: disabled
Radio type: 802.11na
Last packet rate: 300Mb/s (m15 40 MHz)
Last packet RSSI: -45 dBm
Last packet SNR: 50
                            Packets             Bytes
                            -------             -----

Rx Unicast                     1814              2522

Rx Multicast                     68              7846

Rx Encrypt Err                    0                 0

Tx Unicast                     2004           4444900

Rx peak A-MSDU                    6              2048

Rx peak A-MPDU                   13             16345

Tx peak A-MSDU                    6              2048

Tx peak A-MPDU                   13             16345


Queue                    Tx Packets        Tx Dropped       Re-Transmit        Rx Dropped
-------                 -----------       -----------      -----------       -----------

Background                        0                 0                 0                 0

Best Effort                      30                 0                 0                 0
```

```
Queue                  Tx Packets        Tx Dropped       Re-Transmit        Rx Dropped
-------               -----------       -----------       -----------       -----------
Video                            2                 0                 0                 0
Voice                            0                 0                 0                 0

11n Capabilities:
Max Rx A-MSDU size: 2K
Max Rx A-MPDU size: 16K
Max Channel Width: 40MHz
```

For descriptions of the fields of **show sessions network session-id** output, see Table 19– 6 on page 458.

User Name	Up to 30 characters of the name of the authenticated user of this session. **Note:** For a MAC-authenticated session, this value is the client device's MAC address.
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active.
IP or MAC Address	IP address of the session user, or the user's MAC address if the user has not yet received an IP address.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Number of the port and radio through which the user is accessing this session.

Client MAC	MAC address of the session user.
GID	Global session ID, a unique session number within a Mobility Domain.

State	Status of the session: ❑ AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol. ❑ AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated. ❑ AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. ❑ AUTHORIZED—User has been authorized by an AAA method. ❑ ACTIVE—User's AAA attributes have been applied, and the user is active on the network. ❑ DEASSOCIATED—One of the following: • Wireless client has sent the MX switch a disassociate message. • User associated with one of the current MX switch's MP access points has appeared at another MX switch in the Mobility Domain. ❑ ROAMING AWAY—The MX switch has been sent a request to transfer the user, who is roaming, to another MX switch. ❑ STATUS UPDATED—MX switch is receiving a final update from an MP access point about the user, who has roamed away. ❑ WEB_AUTHING—User is being authenticated by WebAAA. ❑ WIRED AUTH'ING—User is being authenticated by the 802.1X protocol on a wired authentication port. ❑ KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a **clear** command, or some other event.
now on	Shows the following information about the MP and radio the session is currently on: ❑ IP address and port number of the MX managing the MP ❑ Serial number and radio number of the MP ❑ Amount of time the session has been on this MP
from	Shows information about the MPs from which the session has roamed. (See the descriptions above for the field.)
Host name	Host name of the user's networking device.
Vlan-Name (and other attributes if set)	Authorization attributes for the user and how they were assigned (the sources of the attribute values). For Vlan-Name, the source of the attribute value can be one of the following: ❑ AAA—VLAN is from RADIUS or the local database. ❑ initial-assignment—For a client that has roamed from one MX to another, VLAN is the one assigned to the user on the MX where the user first accessed the network. (This is the MX where the client's global session in the Mobility Domain started.) This authorization source ( ) is displayed only if the following conditions are true: • The client roamed from another MX. • The service profile for the SSID the user is on is configured to keep the client's initial VLAN assignment. (This means the **keep-initial-vlan** option is enabled on the service profile.) • The VLAN is not configured for the user on the roamed-to switch by the local database. • A Location Policy on the roamed-to MX does not set the VLAN. ❑ location policy—Attribute value was assigned by a Location Policy. ❑ service-profile—Attribute value is configured on the SSID, and was not overridden by other attribute sources (such as AAA or location policy). ❑ Web Portal—Session is for a Web Portal client.

Local Id	Identifier for the session on this particular MX. (This is the session ID you specify when entering the **show sessions network session-i**d command.)
Global Id	Unique session identifier within the Mobility Domain.

Number of packets with encryption errors	Total number of decryption failures.
Number of bytes with encryption errors	Total number of bytes with decryption errors.
Last packet data rate	Data transmit rate, in megabits per second (Mbps), of the last packet received by the MP access point.
Last packet signal strength	Signal strength, in decibels referred to 1 milliwatt (dBm), of the last packet received by the MP access point.
Last packet data S/N ratio	Signal-to-noise ratio of the last packet received by the MP access point.
Protocol	Wireless protocol used.
Session CAC	State of session-based Call Admission Control (CAC) on the SSID's service profile.

See Also **clear sessions network** on page 19-450

MSS automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to a Trapeze device and is not a member of the ignore list

clear rfdetect rogue-list

Removes a MAC address from the attack list.

Syntax **clear rfdetect rogue-list** [*mac-addr* | **all**]

Defaults None.

Access Enabled.

History

Examples The following command clears MAC address 11:22:33:44:55:66 from the rogue list:

```
MX# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer(T)-6()0( rl)-6(ogu )-6(ies)-6st.
```

clear rfdetect neighbor-list

Removes a device from the neighbor list for RF scans. MSS does not generate log messages or traps for the devices in the neighbor list.

Syntax **clear rfdetect neighbor-list [***transmit-mac* **|** *oui* **| all]**

transmit-mac	Basic service set identifier (BSSID), which is a MAC address, of the device to remove from the neighbor list.
oui	A third-party device ID
all	Removes all devices from the neighbor list.

Defaults None.

Access Enabled.

History

MSS Version 3.0	Command introduced.
MSS Version 6.2	Changed **ignore** to **neighbor-list**.

Examples The following command removes BSSID from the neighbor list for RF scans:

```
MX-20# clear rfdetect neighbor-list aa:bb:cc:11:22:33
success: aa:bb:cc:11:22:33 is no longer on the neighbor-list.
```

See Also

- **set rfdetect ignore** on page 20-467
- **show rfdetect neighbor-list** on page 20-476

clear rfdetect ssid-list

Removes an SSID from the permitted SSID list.

Syntax **clear rfdetect ssid-list** *ssid-name*

ssid-name	SSID name you want to remove from the permitted SSID list.

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command clears SSID from the permitted SSID list:

```
MX# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

See Also

- **set rfdetect ssid-list** on page 20-469
- **show rfdetect ssid-list** on page 20-479

set rfdetect active-scan

Deprecated in MSS Version 4.0. You now can disable or reenable active scan in individual radio profiles. See **set radio-profile active-scan** on page 12-256.

set rfdetect rogue-list

Adds an entry to the rogue list. The rogue list specifies the MAC addresses of devices that MSS should issue countermeasures against whenever the devices are detected on the network. The rogue list can contain the MAC addresses of APs and clients.

Syntax **set rfdetect rogue-list** *mac-addr*

mac-addr	MAC address you want to add as a rogue.

Defaults The rogue list is empty by default.

Access Enabled.

History Introduced in MSS Version 4.0.

MSS Version 4.0	Command introduced.
MSS Version 6.2	Command changed from **attack-list** to **rogue-list**.

Usage The rogue list applies only to the MX with the configured list. MX switches do not share rogue lists.

When on-demand countermeasures are enabled (with the **set radio-profile countermeasures configured** command) only those devices configured in the rogue list are subject to countermeasures. In this case, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

Examples The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
MX# set rfdetect rogue-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now in roguelist.
```

See Also

- **clear rfdetect rogue-list** on page 20-462
- **show rfdetect rogue-list** on page 20-470
- **set radio-profile countermeasures** on page 12-265

set rfdetect black-list

Adds an entry to the client blacklist. The client blacklist specifies clients that are not allowed on the network. MSS drops all packets from the clients on the blacklist.

Syntax **set rfdetect black-list** *mac-addr*

mac-addr	MAC address you want to place on the black list.

Defaults The client black list is empty by default.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage In addition to manually configured entries, the list can contain entries added by MSS. MSS can place a client in the blacklist due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the MX with the configured list. MX switches do not share client blacklists.

Examples The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
MX# set rfdetect black-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now blacklisted.
```

See Also

- **set rfdetect black-list** on page 20-465
- **show rfdetect black-list** on page 20-471

set rfdetect classification ad-hoc

Used to classify devices as ad-hoc devices on the network.

Syntax **set rfdetect classification ad-hoc [rogue | skip-test]**

rogue	Detects ad-hoc networks and classifies them as rogues
skip-test	Omit looking for ad-hoc networks and go to the next classification step.

Defaults None

Access Enabled

History Introduced in MSS 6.2

Examples To configure MSS to detect ad-hoc networks and classify them as rogue devices, use the following command:

```
MX>set rfdetect classification ad-hoc rogue
```

set rfdetect classification default

Used to configure the default classification of unknown devices on the network.

Syntax **set rfdetect classification default [rogue | suspect | neighbor]**

rogue	Sets the default classification as rogue.
suspect	Sets the default classification as suspect.
neighbor	Sets the default classification as neighbor.

Defaults None

Access Enabled

History Introduced in MSS 6.2

Examples To configure MSS to detect unknown devices and classify them as rogue devices, use the following command:

```
MX>set rfdetect classification default rogue
```

set rfdetect classification seen-in-network

Used to configure devices seen on the network as rogue devices.

Syntax **set rfdetect seen-in-network [rogue | skip-test]**

rogue	Sets the classification as rogue.
skip-test	

Defaults None

Access Enabled

History Introduced in MSS 6.2

Examples To configure MSS to detect devices seen on the network and classify them as rogue devices, use the following command:

```
MX>set rfdetect classification seen-in-network rogue
```

set rfdetect classification ssid-masquerade

Used to configure devices with spoofed SSIDs as rogue devices.

Syntax **set rfdetect ssid-masquerade [rogue | skip-test]**

Defaults None

Access Enabled

History Introduced in MSS 6.2

Examples To configure MSS to detect unknown devices and classify them as rogue devices, use the following command:

```
MX>set rfdetect classification ssid-masquerade rogue
```

set rfdetect countermeasures

Deprecated in MSS Version 4.0.

set rfdetect countermeasures mac

Deprecated in MSS Version 4.0.

set rfdetect ignore

Deprecated in MSS Version 7.0.

set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

Syntax **set rfdetect log** {**enable** | **disable**}

enable	Enables logging of rogues.
disable	Disables logging of rogues.

Defaults RF detection logging is enabled by default.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage The log messages for rogues are generated only on the seed and appear only in the seed's log message buffer. Use the **show log buffer** command to display the messages in the seed switch's log message buffer.

Examples The following command enables RF detection logging for the Mobility Domain managed by this seed switch:

```
MX-20# set rfdetect log enable
success:  rfdetect logging is enabled.
```

See Also **show log buffer** on page 24-520

set rfdetect signature

Enables MP signatures. An MP signature is a set of bits in a management frame sent by an MP that identifies that MP to MSS. If someone attempts to spoof management packets from a Trapeze MP, MSS can detect the spoof attempt.

Syntax **set rfdetect signature** {**enable** | **disable**}

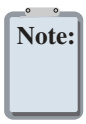
enable	Enables MP signatures.
disable	Disables MP signatures.

Defaults MP signatures are disabled by default.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage The command applies only to MPs managed by the MX switch on which you enter the command. To enable signatures on all MPs in a Mobility Domain, enter the command on each MX switch in the Mobility Domain.



Examples The following command enables MP signatures on an MX:

```
MX-20# set rfdetect signature enable
success:  signature is now enabled.
```

show rfdetect classification

Displays information about the RF detect classifications configured on the network.

Syntax **show rfdetect classification**

Defaults None

Access Enabled

Hist8r[TT6/d

show rfdetect black-list

Displays information abut the clients in the client blacklist.

Syntax **show rfdetect black-list**

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following example shows the client blacklist on MX:

```
MX# show rfdetect black-list
Total number of entries: 1
  Blacklist MAC         Type         Port   TTL
---------------- ----------------- ------- ---
11:22:33:44:55:66 configured        -         -
11:23:34:45:56:67 assoc req flood   3        25
```

See Also

- **clear rfdetect black-list** on page 20-462
- **set rfdetect black-list** on page 20-465

show rfdetect clients

Displays the wireless clients detected by an MX.

Syntax **show rfdetect clients** [**mac** *mac-addr*]

mac *mac-addr* Displays detailed information for a specific client.

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command shows information about all wireless clients detected by an MX and MPs:

```
MX# show rfdetect clients
Total number of entries: 30
Client MAC        Client       AP MAC         AP    Port/Radio    NoL Type  Last
                  Vendor                    Vendor      /Channel            seen
----------------- ------- ----------------- ------- ------------ --- ----- ----

00:03:7f:bf:16:70 Unknown           Unknown            ap 1/1/6     1 intfr 207
00:04:23:77:e6:e5   Intel           Unknown            ap 1/1/2     1 intfr 155
00:05:5d:79:ce:0f  D-Link           Unknown            ap 1/1/149   1 intfr 87
00:05:5d:7e:96:a7  D-Link           Unknown            ap 1/1/149   1 intfr 117
00:05:5d:7e:96:ce  D-Link           Unknown            ap 1/1/157   1 intfr 162
00:05:5d:84:d1:c5  D-Link           Unknown            ap 1/1/1     1 intfr 52
```

The following command displays more details about a specific client:

```
MX# show rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
    Port: ap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago): 84
    Bssid: 00:0b:0e:01:02:00, Vendor: Trapeze, Type: intfr, Dst: ff:ff:ff:ff:ff:ff
    Last Rogue Status Check (secs ago): 3
```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Syntax **show rfdetect countermeasures**

Defaults None.

```
Type                                                Current      Total
--------------------------------------------------- ------------ ------------

Rogue access points                                           0            0
Interfering access points                                   139         1116
Rogue 802.11 clients                                          0            0
Interfering 802.11 clients                                    4          347
802.11 adhoc clients                                          0            1
Unknown 802.11 clients                                       20          965
Interfering 802.11 clients seen on wired network              0            0
802.11 probe request flood                                    0            0
802.11 authentication flood                                   0            0
802.11 null data flood                                        0            0
802.11 mgmt type 6 flood                                      0            0
802.11 mgmt type 7 flood                                      0            0
802.11 mgmt type d flood                                      0            0
802.11 mgmt type e flood                                      0            0
802.11 mgmt type f flood                                      0            0
802.11 association flood                                      0            0
802.11 reassociation flood                                    0            0
802.11 disassociation flood                                   0            0
Weak wep initialization vectors                               0            0
Spoofed access point mac-address attacks                      0            0
Spoofed client mac-address attacks                            0            0
Ssid masquerade attacks                                       1           12
Spoofed deauthentication attacks                              0            0
Spoofed disassociation attacks                                0            0
Null probe responses                                        626        11380
Broadcast deauthentications                                   0            0
FakeAP ssid attacks                                           0            0
FakeAP bssid attacks                                          0            0
Netstumbler clients                                           0            0
Wellenreiter clients                                          0            0
Active scans                                               1796         4383
Wireless bridge frames                                      196          196
Adhoc client frames                                           8            0
Access points present in attack-list                          0            0
Access points not present in ssid-list                        0            0
Access points not present in vendor-list                      0            0
Clients not present in vendor-list                            0            0
Clients added to automatic black-list                         0            0
```

show rfdetect data

Displays information about the APs detected by an MX.

Syntax **show rfdetect data**

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced.
Version 2.0	New option, **verbose**, added to include Trapeze devices and devices in the ignore list.
Version 3.0	❑ , **sentry-sweep**, and **verbose** options deprecated. ❑ Fields rearranged to show BSSID first.

Version 4.0	Vendor, Type, and Flags fields added.
Version 7.0	Added 40 MHz channel information.

Usage You can enter this command on any MX in the Mobility Domain. The output applies only to the MX on which you enter the command. To display all devices that a specific Trapeze radio has detected, even if the radio is managed by another MX, use the **show rfdetect visible** command.

To display rogue information for the entire Mobility Domain, use the **show rfdetect mobility-domain** command on the seed switch.

Only one MAC address is listed for each Trapeze radio, even if the radio is beaconing multiple SSIDs.

Examples The following command shows the devices detected by the MX during the most recent RF detection scan:

```
MX# show rfdetect data
Total number of entries: 197
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor  Type  Port/Radio/Ch Flags  RSSI Age SSID
----------------- ------- ----- ------------- ------ ---- --- -----------------
00:07:50:d5:cc:91   Cisco intfr       3/1/6   i----w  -61   6 r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr       3/1/6   i----w  -82   6 r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr       3/1/2   i-----  -57   6
00:0a:5e:4b:4a:c0    3Com intfr       3/1/11  i-----  -57   6 public
00:0a:5e:4b:4a:c2    3Com intfr       3/1/11  i-t1--  -86   6 trapezewlan
00:0a:5e:4b:4a:c4    3Com intfr       3/1/11  ic----  -85   6 trpz-ccmp
00:0a:5e:4b:4a:c6    3Com intfr       3/1/11  i-t---  -85   6 trpz-tkip
00:0a:5e:4b:4a:c8    3Com intfr       3/1/11  i----w  -83   6 trpz-voip
00:0a:5e:4b:4a:ca    3Com intfr       3/1/11  i-----  -85   6 trpz-webaaa
```

Table 20– 5 describes the fields in this display.

BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: ❑

See Also

- **show rfdetect mobility-domain** on page 20-476
- **show rfdetect visible** on page 20-479

show rfdetect neighbor-list

Displays the BSSIDs of third-party devices that MSS ignores during RF scans. MSS does not

Access Enabled.

History

Usage This command is valid only on the seed MX of the Mobility Domain. To display rogue information for an individual MX, use the **show rfdetect data** command on that MX.

Examples The following command displays summary information for all SSIDs and BSSIDs detected in the Mobility Domain:

```
MX# show rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor       Type  Flags  SSID
----------------- ------------ ----- ------ --------------------------------
00:07:50:d5:cc:91        Cisco intfr i----w r27-cisco1200-2
00:07:50:d5:dc:78        Cisco intfr i----w r116-cisco1200-2
00:09:b7:7b:8a:54        Cisco intfr i-----
00:0a:5e:4b:4a:c0         3Com intfr i----- public
00:0a:5e:4b:4a:c2         3Com intfr i----w trapezewlan
00:0a:5e:4b:4a:c4         3Com intfr ic---- trpz-ccmp
00:0a:5e:4b:4a:c6         3Com intfr i----w trpz-tkip
00:0a:5e:4b:4a:c8         3Com intfr i----w trpz-voip
00:0a:5e:4b:4a:ca         3Com intfr i----- trpz-webaaa
...
```

The following command displays detailed information for a BSSID.

```
MX# show mobility-domain bssid 00:0b:0e:00:04:d1
BSSID: 00:0b:0e:00:04:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Cryy
```

Syntax **show rfdetect visible** *mac-addr*

Syntax **show rfdetect visible ap** *apnum* [**radio** {**1** | **2**}]

mac-addr	Base MAC address of the Trapeze radio. **Note:** To display the base MAC address of a Trapeze radio, use the **show ap status** command.
apnum	Port connected to the MP access point to display neighboring BSSIDs.
radio 1	Shows neighbor information for radio 1.
radio 2	Shows neighbor information for radio 2. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

History

Version 3.0	Command introduced.
Version 4.0	Vendor, Type, and Flags fields added.

Usage If a Trapeze radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

To display rogue information for the entire Mobility Domain, use the **show rfdetect mobility-domain** command on the seed switch.

Examples To following command displays information about the rogues detected by radio 1 on MP port 3:

```
MX# show rfdetect visible ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor  Type  Ch  RSSI Flags  SSID
----------------- ------- ----- --- ---- ------ --------------------------------
00:07:50:d5:cc:91   Cisco intfr   6  -60 i----w r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr   6  -82 i----w r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr   2  -54 i-----
00:0a:5e:4b:4a:c0    3Com intfr  11  -57 i----- public
00:0a:5e:4b:4a:c2    3Com intfr  11  -86 i-t1-- trapezewlan
00:0a:5e:4b:4a:c4    3Com intfr  11  -85 ic---- trpz-ccmp
00:0a:5e:4b:4a:c6    3Com intfr  11  -85 i-t--- trpz-tkip
00:0a:5e:4b:4a:c8    3Com intfr  11  -83 i----w trpz-voip
00:0a:5e:4b:4a:ca    3Com intfr  11  -85 i----- trpz-webaaa
...
```

Table 20– 8 describes the fields in this display.

Transmit MAC	MAC address the rogue device that sent the 802.11 packet detected by the MP radio.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: ❑ rogue—Wireless device that is on the network but is not supposed to be on the network. ❑ intfr—Wireless device not part of your network and is not a rogue, but might be causing RF interference with MP radios. ❑ known—Device that is a legitimate member of the network.
Ch	Channel number on which the radio detected the rogue.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MP radio, in decibels

See Also

- **show rfdetect data** on page 20-474
- **show rfdetect mobility-domain** on page 20-476

Use file management commands to manage system files and to display software and boot information. This chapter presents file management commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Software Version	**reset system** on page 493
	show version on page 500
Boot Settings	**set boot partition** on page 497
	set boot configuration-file on page 496
	set boot backup-configuration on page 496
	show boot on page 497
	clear boot config on page 485
	clear boot backup-configuration on page 484
File Management	**dir** on page 488
	copy on page 485
	md5 on page 492
	delete on page 487
	mkdir on page 492
	rmdir on page 495
Configuration File	**save config** on page 495
	load config on page 491
	on page495

backup

Creates an archive of MX system files and optionally, user file, in Unix ( ) format.

Syntax **backup system** [**tftp:/***ip-addr*/]*filename* [**all** | **critical**]

Defaults The default is **all**.

Access Enabled.

History Introduced in MSS Version 3.2.

Usage You can create an archive located on a TFTP server or in the nonvolatile storage of the MX. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the MX.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the MX. Use the **all** option if you also want to back up or restore WebAAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32 MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the **critical** option instead of the **all** option.

Neither option archives image files or any other files listed in the section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the in the **show boot** command output.) If the running configuration contains unsaved changes, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration currently running on the MX, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.

Examples The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP

See Also

- **set boot backup-configuration** on page 496
- **show boot** on page 497

clear boot config

Resets to the factory default the configuration that MSS loads during a reboot.

Syntax **clear boot config**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples The following commands back up the configuration file on an MX, reset the switch to its factory default configuration, and reboot the MX:

```
MX# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]

MX# clear boot config
success: Reset boot config to factory defaults.

MX# reset system force
...... rebooting ......
```

See Also

- **reset system** on page 493
- **show config** on page 499

copy

Performs the following copy operations:

- Copies a file from a TFTP server to nonvolatile storage.
- Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- Copies a file from one area in nonvolatile storage to another.
- Copies a file to a new filename in nonvolatile storage.

Syntax **copy** *source-url destination-url*

source-url	Name and location of the file to copy. The uniform resource locator (URL) can be one of the following: ❑ [*subdirname*/]*filename* ❑ **file:**[*subdirname*/]*filename* ❑ **tftp://***ip-addr***/**[*subdirname*/]*filename* ❑ **tmp:***filename* For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation. The *subdirname*/ option specifies a subdirectory.
destination-url	Name of the copy and the location to place the copy. The URL can be one of the following: ❑ [*subdirname*/]*filename* ❑ **file:**[*subdirname*/]*filename* ❑ **tftp://***ip-addr***/**[*subdirname*/]*filename* If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following: ❑ **boot0:/***filename* ❑ **boot1:/***filename*

Defaults None.

Access Enabled.

History

Version 1.0	Command introduced
Version 1.1	Enhanced to allow copying files from one area in nonvolatile storage to another and from one name to another in the same area
Version 3.0	Subdirectory support added

Usage The and **file:** URLs are equivalent. You can use either URL to refer to a file in an MX nonvolatile memory. The **tftp://** / URL refers to a file on a TFTP server. If DNS is configured on the MX, you can specify a TFTP server hostname as an alternative to specifying the IP address.

The **tmp:** URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by MSS.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be **boot0** or **boot1**. Enter the filename as **boot0:/** or **boot1:/** . You must specify the boot partition that used to load the currently running image.

The maximum supported file size for TFTP is 32 MB.

Examples The following command copies a file called from nonvolatile storage to a TFTP server:

```
MX# copy floormx tftp://10.1.1.1/floormx
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The following command copies a file called from a TFTP server to nonvolatile storage:

```
MX# copy tftp://10.1.1.1/closetmx closetmx
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

The following command copies system image from a TFTP server to boot partition 1 in nonvolatile storage:

```
MX# copy tftp://10.1.1.107/MX020101.020 boot1:MX020101.020
.....................................................................................
.................success: received 9163214 bytes in 105.939 seconds [ 86495 bytes/sec]
```

The following commands rename to by copying it from one name to the other in the same location, then deleting :

```
MX# copy test-config new-config

MX# delete test-config
success: file deleted.
```

The following command copies file from a TFTP server into subdirectory in an MX switch's nonvolatile storage:

```
MX# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

See Also

- **delete** on page 487
- **dir** on page 488

delete

Deletes a file.

MSS does not prompt you to verify if you want to delete a file. When you press Enter after typing a **delete** command, MSS immediately deletes the specified file.

MSS does not allow you to delete the currently running software image file or the running configuration.

Syntax **delete** *url*

Defaults None.

Access Enabled.

History

Usage You might want to copy the file to a TFTP server as a backup before deleting the file.

Examples The following commands copy file to a TFTP server and delete the file from nonvolatile storage:

```
MX# copy testconfig tftp://10.1.1.1/testconfig
```

```
Boot:
Filename                                        Size          Created
boot0:mx040100.020                             9780 KB      Aug 23 2005, 15:54:08
*boot1:mx040100.020                            9796 KB      Aug 28 2005, 21:09:56
Boot0: Total:        9780 Kbytes used, 2460 Kbytes free
Boot1: Total:        9796 Kbytes used, 2464 Kbytes free
================================================================================
temporary files:
Filename                                        Size          Created
core:command_audit.cur                          37 bytes   Aug 28 2005, 21:11:41
Total:          37 bytes used, 91707 Kbytes free
```

The following command displays the files in the subdirectory:

```
MX# dir old
================================================================================
file:
Filename                                        Size          Created
file:configuration.txt                        3541 bytes   Sep 22 2003, 22:55:44
file:configuration.xml                          24 KB      Sep 22 2003, 22:55:44
Total:          27 Kbytes used, 207824 Kbytes free
```

The following command limits the output to the contents of the user files area:

```
MX# dir file:
================================================================================
file:
Filename                                        Size          Created
file:configuration                              48 KB      Jul 12 2005, 15:02:32
file:corp2:corp2cnfig                           17 KB      Mar 14 2005, 22:20:04
corp_a/                                        512 bytes   May 21 2004, 19:15:48
file:dangcfg                                    14 KB      Mar 14 2005, 22:20:04
dangdir/                                       512 bytes   May 16 2004, 17:23:44
file:pubsconfig-april062005                     40 KB      May 09 2005, 21:08:30
file:sysa_bak                                   12 KB      Mar 15 2005, 19:18:44
file:testback                                   28 KB      Apr 19 2005, 16:37:18
Total:         159 Kbytes used, 207663 Kbytes free
```

The following command limits the output to the contents of the subdirectory:

```
MX# dir core:
================================================================================
file:
Filename                                        Size          Created
core:command_audit.cur                          37 bytes   Aug 28 2005, 21:11:41
Total:          37 bytes used, 91707 Kbytes free
```

The following command limits the output to the contents of the partition:

```
MX# dir boot0:
================================================================================
file:
Filename                                        Size          Created
boot0:mx040100.020                             9780 KB      Aug 23 2005, 15:54:08
Total:        9780 Kbytes used, 207663 Kbytes free
```

Table 21– 1 describes the fields in the **dir** output.

See Also

- **copy** on page 485
- **delete** on page 487

install soda agent

Installs Sygate On-Demand (SODA) agent files in a directory on the MX.

Syntax **install soda agent** *agent-file* **agent-directory** *directory*

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.2.

Usage Use this command to install a .zip file containing SODA agent files into a directory on the MX switch. Prior to installing the SODA agent files, you must have already copied the .zip file to the MX switch. This command creates the specified directory, unzips the file and places the contents into the directory. If the specified directory has the same name as an SSID, then that SSID uses the SODA agent files in the directory if SODA functionality is enabled for the service profile that manages the SSID.

Examples The following command installs the contents of the file into a directory called .

```
MX# install soda agent soda.ZIP agent-directory sp1
```

load config

Loads configuration commands from a file and replaces the MX running configuration with the commands in the loaded file.

Syntax **load config** [*url*]

Defaults The default file location is nonvolatile storage.

If you do not specify a filename, MSS uses the same configuration filename that was used for the previous configuration load. For example, if the MX used for the most recent configuration load, MSS uses again unless you specify a different filename. To display the filename of the configuration file MSS loaded during the last reboot, use the **show boot** command.

Access Enabled.

History

Usage This command completely replaces the running configuration with the configuration in the file.

Examples The following command reloads the configuration from the most recently loaded configuration file:

```
MX# load config
Reloading configuration may result in lost of connectivity, do you wish to continue? (y/n)
[n]y
success: Configuration reloaded
```

The following command loads configuration file :

```
MX# load config testconfig1
Reloading configuration may result in lost of connectivity, do you wish to continue? (y/n)
[n]y
success: Configuration reloaded
```

See Also

- **save config** o/TT12w[(e cled.)]TJiT9.2(l9. 1 Tf9.9e)]ed.

- **show config** on page 499

md5

Calculates the MD5 checksum for a file in the MX nonvolatile storage.

Syntax **md5** [**boot0:** | **boot1:**]*filename*

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

Examples The following command calculates the checksum for image file MX040003.020 in boot partition 0:

```
pubs# md5 boot0:MX040003.020
MD5 (boot0:MX040003.020) = b9cf7f527f74608e50c70e8fb896392a
```

See Also

- **copy** on page 485
- **dir** on page 488

mkdir

Creates a new subdirectory in nonvolatile storage.

Syntax **mkdir** [*subdirname*]

Defaults None.

Access Enabled.

History Introduced in MSS Version 3.0.

Examples The following commands create a subdirectory called and display the root directory to verify the result:

```
MX# mkdir corp2
success: change accepted.

MX# dir
================================================================================
file:
Filename                                    Size          Created
file:configuration                          17 KB      May 21 2004, 18:20:53
```

```
file:dangcfg                                    13 KB      May 16 2004, 18:30:44
dangdir/                                     512 bytes   May 16 2004, 17:23:44
old/                                         512 bytes   Sep 23 2003, 21:58:48
Total:          33 Kbytes used, 207822 Kbytes free
================================================================================
Boot:
Filename                                        Size           Created
*boot0:bload                                   746 KB      May 09 2004, 19:02:16
*boot0:mx030000.020                           8182 KB      May 09 2004, 18:58:16
boot1:mx030000.020                            8197 KB      May 21 2004, 18:01:02
Boot0: Total:        8928 Kbytes used, 3312 Kbytes free
Boot1: Total:        8197 Kbytes used, 4060 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
Total:         0 bytes used, 93537 Kbytes free
```

See Also

- **dir** on page 488
- **rmdir** on page 495

reset system

Restarts an MX and reboots the software.

Syntax **reset system** [**force**]

force	Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Usage If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, MSS does not restart the MX but instead displays a message advising you to either save the configuration changes or use the **force** option.

Examples The following command restarts an MX that does not have any unsaved configuration changes:

```
MX# reset system
This will reset the entire system. Are you sure (y/n)y
```

The following commands attempt to restart an MX switch with a running configuration with unsaved changes, and then force the MX to restart:

```
MX# reset system
error: Cannot reset, due to unsaved configuration changes. Use "reset system force" to
override.
```

```
MX# reset system force
...... rebooting ......
```

See Also

- **save config** on page 495
- **show boot** on page 497

- **show version** on page 500

restore

Unzips a system archive created by the **backup** command and copies the files from the archive onto the switch.

Syntax **restore system** [**tftp:/***ip-addr***/**]*filename* [**all** | **critical**] [**force**]

[**tftp:/***ip-addr***/**]*filename*	Name of the archive file to load. The archive can be located in the MX nonvolatile storage or on a TFTP server.
all	

Defaults The default is **critical**.

Access Enabled.

History Introduced in MSS Version 3.2.

Usage If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the MX. The **restore** command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack an archive from one MX onto another MX.

If the configuration running on the MX is different from the one in the archive or you renamed the configuration file, and you want to retain changes made after the archive was created, see the "Managing System Files" chapter of the .

Examples The following command restores system-critical files on a MX from archive :

```
MX# restore system tftp:/10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386 bytes/sec]
```

```
success: restore complete.
```

See Also **backup** on page 483

rmdir

Removes a subdirectory from nonvolatile storage.

Syntax **rmdir** [*subdirname*]

subdirname	Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults None.

Access Enabled.

History Introduced in MSS Version 3.0.

Usage MSS does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.

Examples The following example removes subdirectory :

```
MX# rmdir corp2
success: change accepted.
```

See Also

- **dir** on page 488
- **mkdir** on page 492

save config

Saves the running configuration to a configuration file.

Syntax **save config** [*filename*]

filename	Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces. To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults By default, MSS saves the running configuration as the configuration filename used during the last reboot.

Access Enabled.

History

Version 1.0	Command introduced
Version 3.0	Subdirectory support added, to save the configuration file to a subdirectory

Usage If you do not specify a filename, MSS replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file MSS loaded during the most recent reboot, use the **show boot** command.

The command completely replaces the specified configuration file with the running configuration.

Examples

History

Usage The file must be located in the MX nonvolatile storage.

Examples The following command sets the boot configuration file to :

```
MX# set boot configuration-file testconfig1
success: boot config set.
```

set boot partition

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

Syntax **set boot partition** {**boot0** | **boot1**}

Defaults By default, an MX uses the same boot partition for the next software reload that was used to boot the currently running image.

Access Enabled.

History Introduced in MSS Version 1.1.

Usage To determine the boot partition used to load the currently running software image, use the **dir** command.

Examples The following command sets the boot partition for the next software reload to partition 1:

```
MX# set boot partition boot1
success: Boot partition set to boot1.
```

See Also

- **copy** on page 485
- **dir** on page 488
- **reset system** on page 493

show boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

Syntax **shTm.00.96-5.4 syste8io.fnlT4 1 Tf8.1356 0 0 9 104.1 15334 Tm-.0032 Tc.0007 TwDefaults**

History

Version 1.0	Command introduced
Version 1.1	The following fields were removed because they are not applicable in 1.1: ❑ Last boot status ❑ Unpacking status
Version 2.1	❑ New field, Product model, added
Version 4.1	❑ New fields, Configured boot version and Backup boot configuration, added

Examples The following command shows the boot information for an MX:

```
MX# show boot
Configured boot version:         4.1.0.65
Configured boot image:           boot1:mx040100.020
Configured boot configuration:   file:configuration
Backup boot configuration:       file:backup.cfg
Booted version:                  4.1.0.65
Booted image:                    boot1:mx040100.020
Booted configuration:            file:configuration
Product model:                   MX
```

Table 21– 2 describes the fields in the **show boot** output.

Configured boot version	Software version the MX runs when the software is rebooted.
Configured boot image	Boot partition and image filename MSS uses to boot when the software is rebooted.
Configured boot configuration	Configuration filename MSS uses to boot when the software is rebooted.
Backup boot configuration	The name of the configuration file to be used in the event that MSS cannot read the configured boot configuration file next time the software is rebooted.
Booted version	Software version the MX is running.
Booted image	Boot partition and image filename MSS used the last time the software was rebooted. MSS is running this software image.
Booted configuration	Configuration filename MSS used to load the configuration the last time the software was rebooted.

See Also

- **clear boot config** on page 485
- **reset system** on page 493
- **set boot configuration-file** on page 496
- **show version** on page 500

show config

Displays the configuration running on the MX.

Syntax **show config** [**area** *area*] [**all**]

area *area* — Configuration area. You can specify one of the following:

- **aaa**
- **acls**
- **ap**
- **ap-trace**
- **arp**
- **eapol**
- **httpd**
- **ip**
- **ip-config**
- **l2acl**
- **load-balancing**
- **log**
- **mobility-domain**
- **network-domain**
- **ntp**
- **port-group**
- **port config**
- **qos**
- **radio-profile**
- **rfdetect**
- **service-profile**
- **sm**
- **snmp**
- **snoop**
- **spantree**
- **system**
- **trace**
- **vlan**
- **vlan-fdb**
- **vlan-profile**

If you do not specify a configuration area, nondefault information for all areas is displayed.

all — Includes configuration items set to the default values.

Defaults None.

Access Enabled.

History

semvl
cham 2g00404110
of os at2500dge
Usage If you do not specify any parameters, configuration commands are set
nondefault values are displayed for dTIf vo v ara,n comma

```
        Copyright (c) 2002, 2003, 2004, 2005 Trapeze Networks, Inc. All rights reserved.

Build Information: (build#67) TOP 2005-07-21 04:41:00
Model:             MX
Hardware
   Mainboard:      version 24 ; revision 3 ; FPGA version 24
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
Flash:             4.1.0.14  - md0a
Kernel:            3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:        4.10 / 4.1.0
```

The following command displays additional software build information and MP information:

```
MX# show version details

        Mobility System Software, Version: 4.1.0 QA 67
        Copyright (c) 2002, 2003, 2004, 2005 Trapeze Networks, Inc. All rights reserved.

Build Information: (build#67) TOP 2005-07-21 04:41:00
Label:             4.1.0.67_072105_MX20
Build Suffix:      -d-O1
Model:             MX
Hardware
   Mainboard:      version 24 ; revision 3 ; FPGA version 24
   CPU Model:      750 (Revision 3.1)
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
Flash:             4.1.0.14  - md0a
Kernel:            3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:        4.10 / 4.1.0

Port/ AP AP Model   Serial #       Versions
-------- ---------- -------------- ------------------------
11  /-   MP-352     0424902948     H/W  : A
                                    F/W1 : 5.6
                                    F/W2 : 5.6
                                    S/W  : 4.1.0.67_072105_0432__AP
                                BOOT S/W : 4.0.3.15_062705_0107__AP
```

Table 21– 3 describes the fields in the **show version** output.

See Also **show boot** on page 497

uninstall soda agent

Removes the contents of a direct

Use trace commands to perform diagnostic routines. While MSS allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces MSS allows, type the **set trace ?** command.

Using the **set trace** command can have adverse effects on system performance. Trapeze Networks recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

This chapter presents trace commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Trace	**set trace sm** on page 22-507
	set trace dot1x on page 22-506
	set trace authentication on page 22-504
	set trace authorization on page 22-505
	show trace on page 22-507
	show trace on page 22-507
	save trace on page 22-504
	clear log trace on page 22-503

clear log trace

Deletes the log messages stored in the trace buffer.

Syntax **clear log trace**

Defaults None.

Access Enabled.

History Introduced in MSS Version 1.0.

Examples To delete the trace log, type the following command:

```
MX# clear log trace
```

See Also

- **set log** on page 24-518
- **show log buffer** on page 24-520

clear trace

Deletes running trace commands and ends trace processes.

Syntax **clear trace** {*trace-area* | **all**} Syntax

Syntax **set trace authentication [ip-addr** *ip address***]** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

ip-addr *ip address*	Specify an IP address in the IPv4 format.
mac-addr *mac-address*	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-num*	Traces a port number. Specify an MX port number between 1 and 22.
user *username*	Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.
level *level*	ide a us-readabl9(e)]T-13.6267 0 TD-.0035 Tc-17359 Tws ftforMXe

Defaults The default trace level is 5.

Access Enabled.

History

History Introduced in MSS Version 1.0.

Examples The following command starts a trace for information about user authentication:

```
MX# set trace authentication user jose
success: change accepted.
```

See Also

- **clear trace** on page 22-503
- **show trace** on page 22-507

set trace authorization

Traces authorization information.

Syntax **set trace authorization [ip-addr** *ip address***]**[**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

Defaults The default trace level is 5.

Access Enabled.

History

MSS Version 1.0	Command introduced.
MSS Version 7.0	The option **ip-addr** was added.

Examples The following command starts a trace for information for authorization for MAC address 00:01:02:03:04:05:

```
MX# set trace authorization mac-addr 00:01:02:03:04:05
success: change accepted.
```

See Also

- **clear trace** on page 22-503
- **show trace** on page 22-507

set trace dot1x

Traces 802.1X sessions.

Syntax **set trace dot1x [ip-addr** *ip address***]**[**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

ip-addr *ip address*	Specify an IP address in the IPv4 format.
mac-addr *mac-address*	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-num*	Traces a port number. Specify an MX port number between 1 and 22.
user *username*	Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
level *level*	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults The default trace level is 5.

Access Enabled.

History

MSS Version 1.0	Command introduced.
MSS Version 7.0	The option **ip-addr** was added.

Examples The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05:

```
MX# set trace dot1x mac-addr 00:01:02:03:04:05:
success: change accepted.
```

See Also

- **clear trace** on page 22-503
- **show trace** on page 22-507

```
------------------- ----- ---------------- ---------------- ---- --------
dot1x                   5                                              0
sm                      5                                              0
```

See Also

- **clear trace** on page 22-503
- **set trace authentication** on page 22-504
- **set trace authorization** on page 22-505
- **set trace dot1x** on page 22-506
- **set trace sm** on page 22-507

Use snoop commands to monitor wireless traffic, by using an MP as a sniffing device. The MP copies the sniffed 802.11 packets and sends the copies to an observer, typically a protocol analyzer such as Ethereal or Tethereal.

(For more information, including setup instructions for the monitoring station, see the “Remotely Monitoring Traffic” section in the “Troubleshooting an MX Switch” chapter of the .)

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Remote monitoring (snooping)	**set snoop** on page 23-510
	show snoop info on page 23-513
	clear snoop on page 23-509
	set snoop map on page 23-511
	show snoop map

clear snoop

Deletes a snoop filter.

Syntax **clear snoop** *filter-name*

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command deletes snoop filter :

```
MX# clear snoop snoop1
```

See Also

- **set snoop** on page 23-510
- **show snoop info** on page 23-513

clear snoop map

Removes a snoop filter from an MP radio.

Examples **clear snoop map** *filter-name* **ap** *apnum*

observer *ip-addr*	Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the MP radio still counts the packets that match the filter.
snap-length *num*	Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. Trapeze Networks recommends specifying a snap length of 100 bytes or less.

Defaults No snoop filters are configured by default.

Access Enabled.

History

Version 4.0	Command introduced
Version 5.0	New Boolean operators: **lt** (less than) and **gt** (greater than). The new options apply to **src-mac**, **dest-mac**, and **host-mac**.
Version 6.0	Direction filter added.

Usage Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- Do not specify an observer that is associated with the MP configured with the snoop filter. This configuration causes an endless cycle of snoop traffic.
- If the snoop filter is running on a Distributed MP, and the MP used a DHCP server in its local subnet to configure the IP information, and the MP did not receive a default router (gateway) address as a result, the observer must also be in the same subnet. Without a default router, the MP cannot find the observer.
- The MP with a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the MP to the observer. If the observer is not present, the MP still sends the snoop packets, which uses bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the MP. These ICMP messages can affect network and MP performance.

Examples The following command configures a snoop filter named that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
MX# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
MX# set snoop snoop2 frame-type eq data mac-pair aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
    observer 10.10.30.3 snap-length 100
```

See Also

- **clear snoop** on page 23-509
- **set snoop map** on page 23-511
- **set snoop mode** on page 23-512
- **show snoop info** on page 23-513
- **show snoop stats** on page 23-514

set snoop map

Maps a snoop filter to a radio on an MP. A snoop filter does not take effect until you map it to a radio and enable the filter.

Examples set snoop map *filter-name* **ap** *apnum* **radio** {**1** | **2**}

```
success: filter 'snoop1' enabled
```

See Also

- **show snoop** on page 23-513
- **show snoop info** on page 23-513
- **show snoop map** on page 23-514
- **show snoop stats** on page 23-514

show snoop

Displays the MP radio mapping for all snoop filters.

Syntax **show snoop**

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage To display the mappings for a specific MP radio, use the **show snoop map** command.

Examples The following command shows the MP radio mappings for all snoop filters configured on an MX switch:

```
MX# show snoop
AP: 3          Radio: 2
        snoop1
        snoop2
AP: 2          Radio: 2
        snoop2
```

See Also

- **clear snoop map** on page 23-509
- **set snoop map** on page 23-511
- **show snoop map** on page 23-514

show snoop info

Shows the configured snoop filters.

Syntax **show snoop** *filter-name*

filter-name Name of the snoop filter.

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Examples The following command shows the snoop filters configured in the examples above:

```
MX# show snoop info
snoop1:
        observer 10.10.30.2 snap-length 100
        all packets
snoop2:
        observer 10.10.30.3 snap-length 100
        frame-type eq data
        mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

See Also

- **clear snoop** on page 23-509
- **set snoop** on page 23-510

show snoop map

Shows the MP radios mapped to a specific snoop filter.

Syntax **show snoop map** *filter-name*

filter-name	Name of the snoop filter.

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage To display the mappings for all snoop filters, use the **show snoop** command.

Examples The following command shows the mapping for snoop filter :

```
MX# show snoop map snoop1
filter 'snoop1' mapping
        AP: 3          Radio: 2
```

See Also

- **clear snoop map** on page 23-509
- **set snoop map** on page 23-511
- **show snoop** on page 23-513

show snoop stats

Displays statistics for enabled snoop filters.

Examples **show snoop stats** [*filter-name* [*ap-num* [**radio** {**1** | **2**}]]]

filter-name	Name of the snoop filter.
ap *ap-num*	Number of an MP to which the snoop filter is mapped.
radio 1	Radio 1 of the MP.
radio 2	Radio 2 of the MP. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

History Introduced in MSS Version 4.0.

Usage The MP retains statistics for a snoop filter until the filter is changed or disabled. The MP then clears the statistics.

Examples The following command shows statistics for snoop filter :

```
MX# show snoop stats snoop1
Filter          AP Radio   Rx Match     Tx Match     Dropped
================================================================
snoop1           3     1            96           4           0
```

Table 23– 1 describes the fields in this display.

Filter	Name of the snoop filter.
AP	MP containing the radio that the filter is mapped.
Radio	Radio to which the filter is mapped.
Rx Match	Number of packets received by the radio that match the filter.
Tx Match	Number of packets sent by the radio that match the filter.
Dropped	Number of packets that matched the filter but that were not copied to the observer due to memory or network problems.

set log

Enables or disables logging of MX and MP events to the MX log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

Syntax **set log** {**buffer** | **console** | **current** | **sessions** | **trace**} [**severity** *severity-level*] [**enable** | **disable**]

set log server *ip-addr* [**port** *port-number*] **severity** *severity-level* [**local-facility** *facility-level*]

buffer	Sets log parameters for the log buffer in nonvolatile storage.
console	Sets log parameters for console sessions.
current	Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.
server *ip-addr*	Sets log parameters for a syslog server. Specify an address in dotted decimal notation.
sessions	Sets the default log values for Telnet sessions. You can set defaults for the following log parameters: ❑ Severity ❑ Logging state (enabled or disabled) To override the session defaults for an individual session, type the **set log** command from within the session and use the **current** option.
trace	Sets log parameters for trace files.
port *port-number*	Sets the TCP port for sending messages to the syslog server. You can specify a number from 1 to 65535. The default syslog port is 514.
severity *severity-level*	Logs events at a severity level greater than or equal to the level specified. Specify onein6 1 Tf6667 9(og4.

Defaults

- Events at the error level and higher are logged to the MX console.
- Events at the error level and higher are logged to the MX system buffer.
- Trace logging is enabled, and debug-level output is stored in the MX trace buffer.

Access Enabled.

History

Version 1.0 Command introduced.

Version 4.2 Option **port** added.

Usage Using the command with only **enable** or **disable** turns logging on or off for the target at all levels. For example, entering **set log buffer enable** with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering **set log buffer disable** with no other keywords turns off all logging to the buffer.

Examples To log only emergency, alert, and critical system events to the console, type the following command:

```
MX# set log console severity critical enable
success: change accepted.
```

See Also

- **show log config** on page 24-521
- **clear log** on page 24-517

set log mark

Configures MSS to generate mark messages at regular intervals. The mark messages indicate the current system time and date. Trapeze Networks can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

Syntax **set log mark** [**enable** | **disable**] [**severity** *level*] [**interval** *interval*]

enable	Enables the mark messages.
disable	Disables the mark messages.
severity *level*	Log severity at which the messages are logged: ❑ **emergency** ❑ **alert** ❑ **critical** ❑ **error** ❑ **warning** ❑ **notice** ❑ **info** ❑ **debug**
interval *interval*	Interval at which MSS generates the mark messages. You can specify from 1 to 2147483647 seconds.

Defaults Mark messages are disabled by default. When messages are enabled, MSS generates a message at the notice level once every 300 seconds by default.

Access Enabled.

History Introduced in MSS Version 4.1.

Examples The following command enables mark messages:

```
MX# set log mark enable
```

```
MX#
```

Syntax **show log trace** [{**+**|**-**|**/**}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

trace	Displays the log messages in the trace buffer.
+|**-**|**/** *number-of-messages*	Displays the number of messages specified as follows: ❑ A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log. ❑ A negative number (for example, **-100**) displays that number of log entries starting from newest in the log. ❑ A number preceded by a slash (for example, **/100**) displays that number of the most recent log entries in the log, starting with the least recent.
facility *facility-name*	Area of MSS that is sending the log message. Type a space and a question mark **(?)** after **show log trace facility** for a list of valid facilities.
matching *string*	Displays messages that match a string—for example, a username or IP address.
severity *severity-level*	Displays messages at a severity level greater than or equal to the level specified. Specify one of the following: ❑ **emergency**—The MX switch is unusable. ❑ **alert**—Action must be taken immediately. ❑ **critical**—You must resolve the critical conditions. If the conditions are not resolved, the MX can reboot or shut down. ❑ **error**—The MX is missing data or is unable to form a connection. ❑ **warning—**A possible problem exists. ❑ **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required. ❑ **info**—Informational messages only. No problem exists. ❑ **debug**—Output from debugging.

Defaults None.

Access Enabled.

History

Vet Coettroduced:

Examples Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
MX# show log trace facility ?
<facility name>             Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP, ASO, BOOT,
CLI, CLUSTER, CRYPTO, DOT1X, ENCAP, ETHERNET, GATEWAY, HTTPD, IGMP, IP, MISC, NOSE, NP,
RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE, SYS, TAGMGR, TBRIDGE, TCPSSL,
TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MP, RAPDA, WEBVIEW, EAP, PORTCONFIG, FP.
```

The following command displays the newest five trace log entries for the ROGUE facility:

```
MX# show log trace +5 facility ROGUE
ROGUE Oct 28 16:30:19.695141 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:ff:00:3b Po
rt 7 Radio 1 Chan 36 RSSI 18 Tech DOT_11A SSID trapeze
                                                    ROGUE Oct 28 16:30:19.7046
37 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:00:09:5f Port 7 Radio 1 Chan 36 RSSI
15 Tech DOT_11A SSID examplewlan
                                ROGUE Oct 28 16:30:19.711253 ERROR ROGUE_AP_ALER
T: Xmtr Mac 01:0b:0e:00:06:b7 Port 7 Radio 1 Chan 36 RSSI 36 Tech DOT_11A SSID wlan-7
       ROGUE Oct 28 16:30:19.717954 ERROR ROGUE_AP_ALERT: Xmtr Mac 00:0b:0e:00:0
6:8f Port 7 Radio 1 Chan 36 RSSI 13 Tech DOT_11A SSID trapeze
                                                          ROGUE Oct 28 16:30:
19.727069 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:da:da:dd Port 7 Radio 1 Chan 3
```

```
6 RSSI 22 Tech DOT_11A SSID trapeze
```

See Also

- **clear log** on page 24-517
- **show log config** on page 24-521

OFFDisables the autoboot option.**off**Same effect as **OFF**.**BT=***type*Boot type:

Defaults The autoboot option is enabled by default.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Examples The following command displays the current setting of the autoboot option:`boot> autoboot`
`The autoboot flag is on.`

See Also **boot** on page 25-526

boot

Loads and executes a system image file.

Syntax **boot** [**BT=***type*] [**DEV=***device*] [**FN=***filename*] [**HA=***ip-addr*] [**FL=***num*] [**OPT=***option*] [**OPT+=***optio*

- **c**—Compact flash. Boots using nonvolatile storage or a flash card.
- **n**—Network. Boots using a TFTP server.**DEV=***device*Location of the system image file:

- **c:**—Nonvolatile storage area containing boot partition 0
- **d:**—Nonvolatile storage area containing boot partition 1
- **e:**—Primary partition of the flash card in the flash card slot
- **f:**—Secondary partition of the flash card in the flash card slot
- **boot0**—boot partition 0
- **boot1**—boot partition 1When the boot type is **n** (network), the device can be one of the following:

- **emac1**—Port 1 on an MXR-2
- **emac2**—Port 2 on an MXR-2
- **mgmt** or **tsec0**—The 10/100 port labelled Mgmt on an MX-200 or MX-216**FN=***filename*System image

Defaults The boot settings in the currently active boot profile are used by default.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage If you use an optional parameter, the parameter setting overrides the setting of the same parameter in the currently active boot profile. However, the boot profile itself is not changed. To display the currently active boot profile, use the **show** command. To change the currently active boot profile, use the **change** command.

Examples The following command loads system image file MX010101.020 from boot partition 1:

```
boot> boot FN=MX010101.020 DEV=boot1
Compact Flash load from boot1:testcfg matches MX010101.020.
unzip: Inflating ramdisk_1.1.1.. OK
unzip file len 36085486 OK


Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003
    The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California.  All rights reserved.

Power Cycle Reboot
Detecting hardware...done.
readclock: 2003-10-8 2:9:50.67 UTC=>1065578990.670000 (1064992894)
init: Creating mfs /dev
erase ^H, werase ^W, kill ^U, intr ^C, status ^T
Doing Trapeze mounts and links
Starting nos_mon...
        nos_mon:ps: not found
SYSLOGD Oct 08 02:10:05.477814 CRITICAL SYSTEM_READY: The system has finished booting.

Copyright (c) 2002, 2003
        Trapeze Networks, Inc.



Username:
Password:
```

See Also

- **change** on page 25-527
- **show** on page 25-534

change

Changes parameters in the currently active boot profile. (For information about boot profiles, see **show** on page 25-534.)

Syntax **change**

Defaults The default boot type is **c** (compact flash). The default filename is . The default flags setting is 0x00000000 (all flags disabled) and the default options list is run=nos;boot=0. The default device setting is the boot partition specified by the most recent **set boot partition** command typed at the Enabled level of the CLI, or boot 0 if the command has never been typed.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Examples The following command creates a new boot profile in slot 1 on an MX that currently has only one boot profile, in slot 0:

```
boot> create

    BOOT Index:   1
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

See Also

- **change** on page 25-527
- **delete** on page 25-529
- **next** on page 25-533
- **show** on page 25-534

delete

Removes the currently active boot profile. (For information about boot profiles, see **show** on page 25-534.)

Syntax **delete**

Defaults None.

Access Boot prompt.

History Introduced in MSS V6T4aon 1.0.

Usage When you type the **delete** command, the next-lower numbered boot profile becomes the active profile. For example, if the currently active profile is number 3, profile number 2 becomes active after you type **delete** to delete profile 3. You cannot delete boot profile 0.

Examples To remove the currently active boot profile, type the following command:

```
boot> delete

    BOOT Index:   1
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

See Also

- **change** on page 25-527
- **create** on page 25-528
- **next** on page 25-533
- **show** on page 25-534

dhcp

Displays or changes the state of the DHCP optaon. The DHCP optaon controls whether an MX uses DCHP to obtain its IP address when it is booted using a TFTP server.

Syntax **dhcp** [**ON** | **on** | **OFF** | **off**]

ON	Enables the DHCP option.
on	Same effect as **ON**.
OFF	Disables the DHCP option.
off	Same effect as **OFF**.

Defaults The DHCP option is disabled by default.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Examples The following command displays the current setting of the DHCP option:

```
boot> dhcp
DHCP is currently enabled.
```

The following command disables the DHCP option:

```
boot> dhcp
DHCP is currently disabled.
```

See Also **boot** on page 25-526

diag

Accesses the diagnostic mode.

Syntax **diag**

Defaults The diagnostic mode is disabled by default.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage Access to the diagnostic mode requires a password, which is not user configurable. Use this mode only if advised to do so by Trapeze Networks.

dir

Displays the boot code and system image files on an MX switch.

Syntax **dir** [**c:** | **d:** | **e:** | **f:** | **boot0** | **boot1**]

c:	Nonvolatile storage area containing boot partition 0 (primary).
d:	Nonvolatile storage area containing boot partition 1 (secondary).
e:	Primary partition of the flash card in the flash card slot.
f:	Secondary partition of the flash card in the flash card slot.
boot0	Boot partition 0.
boot1	Boot partition 1.

Defaults None.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage To display the system image software versions, use the **fver** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Examples The following command displays all the boot code and system image files on an MX switch:

```
boot> dir

  Internal Compact Flash Directory (Primary):
        MX010101.020                5523634 bytes
               BLOAD                 696176 bytes
              BSTRAP                  38056 bytes

  Internal Compact Flash Directory (Secondary):
        MX010101.020                5524593 bytes
```

See Also

- **fver** on page 25-531
- **version** on page 25-536

fver

Syntax **help** [*command-name*]

command-name Boot prompt command.

Defaults None.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage If you specify a command name, detailed information is displayed for that command. If you do not specify a command name, all the boot prompt commands are listed.

Examples The following command displays detailed information for the **fver** command:

```
boot> help fver

        fver  Display the version of the specified device:filename.

  USAGE:  fver [c:file|d:file|e:file|f:file|boot0:file|boot1:file|boot2:file|boo
t3:file]

    Command to display the version of the compressed image file
    associated with the given device:filename.
```

See Also **ls** on page 25-532

ls

Displays a list of the boot prompt commands.

Syntax **ls**

Defaults None.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage To display help for an individual command, type help followed by the command name (for example, **help boot**).

Examples To display a list of the commands available at the boot prompt, type the following command:

```
boot> ls
          ls     Display a list of all commands and descriptions.
        help     Display help information for each command.
    autoboot     Display the state of, enable, or disable the autoboot option.
        boot     Load and execute an image using the current boot configuration profile.
      change     Change the current boot configuration profile.
      create     Create a new boot configuration profile.
      delete     Delete the current boot configuration profile.
        next     Select the next boot configuration profile.
        show     Display the current boot configuration profile.
         dir     Display the contents of the specified boot partition.
        fver     Display the version of the loadable image specified by device:filename.
     version     Display HW and Bootstrap/Bootloader version information.
       reset     Reset the system.
        test     Display the state of, enable, or disable the tests option.
        diag     Access the diagnostic command CLI.
```

See Also **help** on page 25-531

next

Activates and displays the boot profile in the next boot profile slot. (For information about boot profiles, see **show** on page 25-534.)

Syntax **next**

Defaults None.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage An MX contains 4 boot profil

```
Trapeze Networks MX Bootstrap/Bootloader

                  Version  1.6.5  Release
     Bootstrap 0 version:          1.17     Active
    Bootloader 0 version:         1.6.5     Active
     Bootstrap 1 version:          1.17
    Bootloader 1 version:         1.6.3

       MX Board Revision:    3.
  MX Controller Revision:    24.
      POE Board Revision:    1
 POE Controller Revision:    6

    BOOT Index:   0
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

See Also **boot** on page 25-526

show

Displays the currently active boot profile. A boot profile is a set of parameters that an MX uses to control the boot process. Each boot profile contains the following parameters:

- Boot type—Either compact flash (local device on the MX) or network (TFTP)
- Boot device—Location of the system image file
- Filename—System image file
- Flags—Number representing the bit settings of boot flags to pass to the booted system image.
- Options—String up to 128 bytes of boot options to pass to the booted system image

An MX can have up to four boot profiles, numbered 0 through 3. Only one boot profile can be active at a time. You can create, change, and delete boot profiles. You also can activate another boot profile in place of the currently active one.

Syntax **show**

Defaults None.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Examples To display the currently active boot profile, type the following command at the boot prompt:

```
boot> show

    BOOT Index:   0
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

The following is an example of a boot profile from an MXR-2 that is booted with a software image downloaded from a TFTP server. In the example, when the MXR-2 boots, it downloads a system image file called located on a TFTP server with address 172.16.0.1.

```
boot> show

    BOOT Index:   0
    BOOT TYPE:    n
    DEVICE:       emac1
    FILENAME:     bootfile
    HOST IP:      172.16.0.1
    LOCAL IP:     172.16.0.21
    GATEWAY IP:   172.16.0.20
    IP MASK:      255.255.255.0
    FLAGS:        00000000
    OPTIONS:      run=nos
```

Table 25– 1 describes the fields in the display.

BOOT Index	Boot profile slot, which can be a number from 0 to 3.
BOOT TYPE	Boot type: ❑ **c**—Compact flash. Boots using nonvolatile storage or a flash card. ❑ **n**—Network. Boots using a TFTP server.
DEVICE	Location of the system image file: ❑ **c:**—Nonvolatile storage area containing boot partition 0 ❑ **d:**—Nonvolatile storage area containing boot partition 1 ❑ **e:**—Primary partition of the flash card in the flash card slot ❑ **f:**—Secondary partition of the flash card in the flash card slot ❑ **boot0**—boot partition 0 ❑ **boot1**—boot partition 1 When the boot type is Network, the device can be one of the following: ❑ **emac1**—Port 1 on an MXR-2 ❑ **emac2**—Port 2 on an MXR-2 ❑ **mgmt** or

See Also

- **change** on page 25-527
- **create** on page 25-528
- **delete** on page 25-529
- **dhcp** on page 25-529
- **next** on page 25-533

test

Displays or changes the state of the poweron test flag. The poweron test flag controls whether an MX performs a set of self tests prior to the boot process.

Syntax **test** [**ON** | **on** | **OFF** | **off**]

ON	Enables the poweron test flag.
on	Same effect as **ON**.
OFF	Disables the poweron test flag.
off	Same effect as **OFF**.

Defaults The poweron test flag is disabled by default.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Examples The following command displays the current setting of the poweron test flag:

```
boot> test
The diagnostic execution flag is not set.
```

See Also **boot** on page 25-526

version

Displays version information for the MX hardware and boot code.

Syntax **version**

Defaults None.

Access Boot prompt.

History Introduced in MSS Version 1.0.

Usage This command does not list the system image file versions installed in the boot partitions. To display system image file versions, use the **dir** or **fver** command.

Examples To display hardware and boot code version information, type the following command at the boot prompt:

```
boot> version

    Trapeze Networks MX Bootstrap/Bootloader

                 Version  1.6.5  Release
     Bootstrap 0 version:          1.17     Active
    Bootloader 0 version:         1.6.5     Active
     Bootstrap 1 version:          1.17
    Bootloader 1 version:         1.6.3

       MX Board Revision:    3.
  MX Controller Revision:    24.
      POE Board Revision:    1
 POE Controller Revision:    6
```

See Also

- **dir** on page 25-530
- **fver** on page 25-531