# Mobility System Software User's Guide
# Version 7.0

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

- 
- 
- 
- 
- **show tech-support**
- 
- 
- 

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:

**a.** Repair and return of the defective hardware;

**b.** Replace the defective hardware with a new or refurbished component;

**c.** Replace the defective hardware with a different but similar component that contains compatible features and functions; or

**d.** 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 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 environmen TD-.00054.3(oeo3e-7w6(h)-3.8(

IN NO EVENT SHALL TRAPEZE NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED RESELLERS BE LIABLE TO CUSTOMER OR ANY THRID PARTY FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES REGARDLESS OF HOW THOSE DAMAGES WERE CAUSED. NOR WILL TRAPEZE NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED RESELLERS BE 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 software, and will include the Trapeze NetwoiYRDAMNumb tios

1

# About This Guide

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 enter on a Mobility Exchange™.

Read the documentation set if you are a network administrator responsible for managing Mobility Exchange (MX) switches and Mobility Point™ (MP™) access points in a network.

## Trapeze Networks Mobility System

The Trapeze Networks Mobility System is an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The Trapeze system provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices.

The Trapeze Mobility System fulfills the three fundamental requirements of an enterprise WLAN: It eliminates the distinction between wired and wireless networks, allows users to work safely from anywhere ( ), and provides a comprehensive suite of intuitive tools for planning and managing the network before and after deployment, greatly easing the operational burden on IT resources.

The Trapeze Networks Mobility System consists of the following components:

- **RingMaster tool suite**— A full-featured graphical user interface (GUI) application used to plan, configure, deploy, and manage a WLAN and its users
- **One or more Mobility Exchange™ (MX™) switches**— Distributed, intelligent machines for managing user connectivity, connecting and powering Mobility Point (MP) access points, and connecting the WLAN to the wired network backbone
- **Multiple Mobility Point™ (MP™) access points**— Wireless access points (APs) that transmit and receive radio frequency (RF) signals to and from wireless users and connect them to an MX switch
- **Mobility System Software™ (MSS™)**— The operating system that runs all MX switches and MPs in a WLAN, and is accessible through a command-line interface (CLI), the Web View interface, or the RingMaster GUI.

## Documentation

Consult the following documents to plan, install, configure, and manage a Trapeze Networks Mobility System.

### Planning, Configuration, and Deployment

- — Instructions for installing and configuring RingMaster services.
- — Instructions for planning, deploying, and managing the entire WLAN with the RingMaster tool suite. Read this guide to learn how to plan wireless services.
- — Instructions for configuring the WLAN with the RingMaster tool suite. Read this guide to learn how to configure wireless services.
- — Instructions for managing and monitoring your WLAN using the RingMaster tool suite and how to optimize and manage your WLAN.

## Installation

- — Instructions and specifications for installing an MX.
- — 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.

## Configuration and Management

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

## Safety and Advisory Notices

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


This situation or condition can lead to data loss or damage to the product or other property.


### Hypertext Links

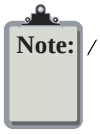
Hypertext links appear in Blue.

As an example, this is a link to **Contacting the Technical Assistance Center**.

## Text and Syntax Conventions

Trapeze guides use the following text and syntax conventions:

| Convention | Use |
|---|---|
| | Sets off command syntax or sample commands and system responses. |
| **Bold text** | Highlights commands that you enter or items you select. |
| | Designates command variables that you replace with appropriate values or highlights publication titles or words requiring special emphasis. |
| ***Bold italic text font*** | ***Bold italic text font*** in narrative, capitalized or not, indicates a program name, function name, or string. |
| **Menu Name** > **Command** | Indicates a menu item. For example, **File** > **Exit** indicates that you select **Exit** from the **File** menu. |
| (square brackets) | Enclose optional parameters in command syntax. |
| (curly brackets) | Enclose mandatory parameters in command syntax. |
| (vertical bar) | Separates mutually exclusive options in command syntax. |




/

## Information Required When Requesting Service

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

- Your company name and address
- Your name, phone number, cell phone or pager number, and e-mail address
- Name, model, and serial number of the product(s) requiring service
  - 
- Output of the ***show tech-support*** command
- Wireless client information
  - 
  - 
- 

## Limited Warranty for Hardware and Software

TERMS AND CONDITIONS OF SALE

**1.** Software

Any software provided is lice

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:

- Use reasonable commercial efforts to attempt to correct or provide workarounds for errors;
- Replace the software with functionally equivalent software; or
- 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 WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM JURISDICTION TO JURISDICTION. THE LIMITED WARRANTY ABOVE IS THE SOLE REMEDY FOR ANY BREACH OF ANY WARRANTY WITH RESPECT TO THE HARDWARE AND SOFTWARE AND IS IN LIEU OF ANY AND ALL OTHER REMEDIES.

7. Limitation of Liabilities

   IN NO EVENT SHALL TRAPEZE NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED RESELLERS BE LIABLE TO CUSTOMER OR ANY THRID PARTY FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES REGARDLESS OF HOW THOSE DAMAGES WERE CAUSED. NOR WILL TRAPEZE NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED RESELLERS BE 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 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.**

# 2

# Using the Command-Line Interface

Mobility System Software (MSS) supports a Trapeze Networks Mobility System wireless LAN (WLAN) consisting of RingMaster software, Mobility Exchange (MX) switches, and Mobility Point (MP) access points. MSS has a command-line interface (CLI) on the MX that you can use to configure and manage the MX and the attached MPs.

You configure the MX and the MP primarily with **set**, **clear**, and **show** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command. Use **show** commands to display the current configuration and monitor the status of network operations.

The MX supports two connection modes:

- Administrative access mode, which enables the network administrator to connect the MX and configure the network.
- Network access mode, which enables network users to connect the MX to access the network

## CLI Conventions

Be aware of the following MSS CLI conventions for command entry:



### Command Prompts

By default, the MSS CLI provides the following prompt for restricted users. The portion shows the MX model number (for example, ) and the portion shows the last 6 digits of the MX media access control (MAC) address.

When you log into the MX as an administrative user and enter the **enable** command and supplying a suitable password, MSS displays the following prompt:

For ease of presentation, this manual shows the restricted and enabled prompts as follows:

For information about changing the CLI prompt on an MX, see the **set prompt** command description in the .

## Syntax Notation

The MSS CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:

  **set enablepass**

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

  **clear interface ip**

- 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:

  **clear fdb dynamic port vlan**

- 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:

  **set port enable disable**

## Text Entry Conventions and Allowed Characters

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.

It is recommended 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

### Wildcard Masks

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine if the MX filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any s (zeros) in the mask, but does not check the bits that correspond to s (ones) in the mask. Specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

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.

## Port Lists

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 single port or multiple ports in a command that includes **port** . Use one of the following formats for :

- A single port number. For example:

  **set port enable 16**

- A comma-separated list of port numbers, with no spaces. For example:

  **show port poe 1,2,4,13**

- A hyphen-separated range of port numbers, with no spaces. For example:

  **reset port 12-16**

- Any combination of .00[(Using the Com]TJ)-4.7(m-.3Com]TJmb)-6.6(em0 TD-.00[(Using the Com]TJ)-4.7(m-.3Com]TJmb)-6.6(em0 TD-.0059 4w[(m)-7.4(n)1.8

| Keyboard Shortcut(s) | Function |
|---|---|
| Ctrl+A | Jumps to the first character of the command line. |
| Ctrl+B or Left Arrow key | Moves the cursor back one character. |
| Ctrl+C | Escapes and terminates prompts and tasks. |
| Ctrl+D | Deletes the character at the cursor. |
| Ctrl+E | Jumps to the end of the current command line. |

## History Buffer

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.

## Tabs

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:

```
MX# show i < ab>
igmp       Show igmp information
interface  Show interfaces
ip         Show ip information
```

## Single-Asterisk (*) Wildcard Character

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

Double-Asterisk (**) Wildcard Characters

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

## User Globs, MAC Address Globs, and VLAN Globs

“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 in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

## User 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 deli hter characters match usernames. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a deli hter character in the glob. Valid user glob deli hter characters are the (@) sign and the period (.).

For example, the following globs identify the following users:

| User Glob | User(s) Designated |
|---|---|
| jose@example.com | User at example.com |
| *@example.com | All users at example.com whose usernames do not contain periods—for example, jose@example.com and tamara@example.com, but nin.wong@example.com, because nin.wong contains a period |
| *@marketing.example.com | All marketing users at example.com whose usernames do not contain periods |
| *.*@marketing.example.com | All marketing users at example.com whose usernames contain a period |
| * | All users with usernames that have no deli hters |
| EXAMPLE* | All users in the Windows Domain EXAMPLE with usernames that have no deli hters |
| EXAMPLE*.* | All users in the Windows Domain EXAMPLE whose usernames contain a period |
| ** | All users |

## MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identhty (OUI).

## VLAN Globs

A VLAN glob is a method for matching one of a set of local rules on an MX, known as the location policy, to one or more users. MSS compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine if the rule applies.

To match VLANs, use the double-asterisk (**) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*) wildcard. Valid VLAN glob delimiter characters are the (@) sign and the period (.).

For example, the VLAN glob matches and and all other VLAN names with at the beginning.

3

# Managing System Files

You can manage files stored on the MX in nonvolatile storage using MSS. In addition, you can copy files between the MX and a TFTP or FTP server on the network.

## About System Files

Generally, the nonvolatile storage of an MX contains the following types of files:

- System image files— Operating system software for the MX and the attached MPs.
- Configuration files—CLI commands that configure the MX and the attached MPs.
- System log files—Files containing log entries generated by MSS.

When you power on or reset the MX or reboot the software, the MX loads a designated system image, then loads configuration information from a designated configuration file.

An MX can also contain temporary files with trace information used for troubleshooting.

```
Flash:              7.0.0.5  - md0a
Kernel:             3.0.0#14: Sat Oct  7 00:03:52 PD  2008
BootLoader:         7.0 / 7.0.6

AP    AP Model    Serial #       Versions
----- ---------- ------------- ------------------------
2     MP-422      0771502184     H/W  : A
                         F/W1 : 7.8
                         F/W2 : 10.4
                         S/W  : 7.0.0.0.143_100107_0012_build
                    BOO  S/W  : 7.0.0.0.143_100107_0012_build
                   fingerprint : (null)
```

(For additional information about the output, see the
)

## Displaying Boot Information

Boot information consists of the MSS version and the names of the system image file and current configuration file on the MX. The **boot** command also lists the system image and configuration file that are loaded after the next reboot. The currently running versions are listed in the Booted fields. The versions that are used after the next reboot are listed in the Configured fields.

To display boot information, type the following command:

```
MX# show boot
MXR2_desk# show boot
Configured boot version:          7.0.0.0.85
Configured boot image:            boot1:mx06000.002
Configured boot configuration:    file:configuration
Backup boot configuration:        file:backup.cfg
Booted version:                   7.0.0.0.85
Booted image:                     boot1:mx06200.002
Booted configuration:             file:configuration
Product model:                    MXR-2
```

In this example, the MX is running software version 7.0.0.0.85. The MX used the image file in boot partition boot1 and the configuration file for the most recent reboot. The MX is set to use image file in boot partition boot1 and configuration file for the next reboot. If MSS cannot read the

The file and boot areas are in nonvolatile storage and remain in storage following a software reload or power cycle. The files in the temporary area are removed following a software reload or power cycle.

The boot area is divided into two partitions: boot0 and boot1. Each partition can contain one sy4.4(e)-u(7oema-)3.9gme iy4.415(l.e)-51(e )]TJ0 -1.6024 TD.0026 Tc-.0033 Tw[(Thefi)4.3(i)-1.7liead n connsub .( 6(Inea)]TJ0 -1.6024 TD.0121 Tc-.0062 Tw[(The)-4.3(i)-1.7(le)-4.3(s)-4.3( )-4.3(in)-4.3( )-4.3(the)-4.3( )-4.3(temporary)-4.3( )-4.3(file)-4.3( )-4.3(system)-4.3( )-4.3(are)-4.3( )-4.3(removed)-4.3( )-4.3(when)-4.3( )-4.3(the)-4.3( )-4.3(system)-4.3( )-4.3(is)-4.3( )-4.3(reloaded)-4.3( )-4.3(or)-4.3( )-4.3(power)-4.3( )-4.3(is)-4.3( )-4.3(cycled.)]TJ0 -1.7 s

```
file:
Filename                                        Size           Created
core:command_audit.cur                          37 bytes   Aug 28 2005, 21:11:41
 otal:          37 bytes used, 91707 Kbytes free
 he following command limits the output to the contents of the boot0 partition:
MX# dir boot0:
================================================================================
file:
Filename                                        Size           Created
boot0:mx040100.020                             9780 KB      Aug 23 2005, 15:54:08
 otal:        9780 Kbytes used, 207663 Kbytes free
```

(For information about the fields in the output, see the )

## Copying a File

You can perform the following copy operations:

- Copy to nonvolatile storage from a TFTP server or FTP server.
- Copy from nonvolatile storage or temporary storage to a TFTP server or FTP server.
- Copy from one area in nonvolatile storage to another.
- Copy a file to a new filename in nonvolatile storage.

To copy a file, use the following command.

```
copy source-url destination-url
```

A URL can be one of the following:

- [ /]
- **file:**[ /]
- **tftp://** /[ /]
- **ftp**:// : @ /
- **tmp:**

The and **file:** URLs are equivalent. You can use either URL to refer to a file on the MX .

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 refers to a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage.

The / option specifies a subdirectory.

If you are copying a system image file into nonvolatile storage, the must include the boot partition name. You can specify one of the following:

- **boot0:/**
- **boot1:/**

You must specify the boot partition that used to load the current image.

The maximum supported file size for TFTP is 32 MB.


You can copy a file from an MX to a TFTP server or from a TFTP server to an MX, but you cannot use MSS to copy a file directly from one TFTP server to another.

To copy the file from nonvolatile storage to a TFTP server, type the following command:

```
MX# copy floor2mx tftp://10.1.1.1/floor2mx
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The above command copies the file to the same filename on the TFTP server. To rename the file, type the following command:

```
MX# copy floor2mx tftp://10.1.1.1/floor2mx-backup
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

To copy a file named from a TFTP server to nonvolatile storage, type the following command:

```
MX# copy tftp://10.1.1.1/newconfig newconfig
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

The above command copies the file to the same filename. To rename the file, type the following command:

```
MX# copy tftp://10.1.1.1/newconfig mxconfig
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

To copy system image from a TFTP server to boot partition 1 in nonvolatile storage, type the following command:

```
MX# copy tftp://10.1.1.107/MX010101.020 boot1:MX010101.020
.....................................................................................
         .........................success: received 9163214 bytes in 105.939 seconds
         [ 86495 bytes/sec]
```

To rename to , you can copy it from one name to the other in the same location, and then delete . Type the following commands:

```
MX# copy test-config new-config
MX# delete test-config
success: file deleted.
```

To copy file from a TFTP server into subdirectory in the nonvolatile storage of the MX, type the following command:

```
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]
```

To copy a file from an FTP server, use the following command:

```
MX# copy ftp://anonymous:password@10.1.1.1/configuration/corpa-login.html
```

## Deleting a File


MSS does not prompt you to verify file deletion. When you press Enter after typing a **delete** command, MSS immediately deletes the specified file. Trapeze Networks recommends that you copy a file to a TFTP server before deleting the file.


MSS does not allow you to delete the currently running software image file or the running configuration.

To delete a file, use the following command:

`delete` *`url`*

The URL can be a filename of up to 128 alphanumeric characters.

To copy a file named to a TFTP server and delete the file from the MX, type the following commands:

```
MX# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

```
MX# delete testconfig
success: file deleted.
```

### Creating a Subdirectory

You can create subdirectories in the user files area of the MX. To create a subdirectory, use the following command:

```
mkdir [subdirname]
```

To create a subdirectory called and display the root directory to verify the result, type the following commands:

```
MX# mkdir corp2
success: change accepted.
MX# dir
================================================================================
file:
Filename                                        Size           Created
file:configuration                               17 KB      May 21 2004, 18:20:53
file:configuration.txt                          379 bytes   May 09 2004, 18:55:17
corp2/                                         512 bytes   May 21 2004, 19:22:09
corp_a/                                        512 bytes   May 21 2004, 19:15:48
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
 otal:          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:  otal:        8928 Kbytes used, 3312 Kbytes free
Boot1:  otal:        8197 Kbytes used, 4060 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
 otal:         0 bytes used, 93537 Kbytes free
```

### Removing a Subdirectory

To remove a subdirectory from the MX, use the following command:

```
rmdir [subdirname]
```

To remove subdirectory , type the following example:

```
MX# rmdir corp2
success: change accepted.
```

## Managing Configuration Files

A configuration file contains CLI commands to set up the MX. The MX loads a designated configuration file immediately after loading the eateaadwhene:ea (ea)5t3.5(t)01 T2 Tc Y (ea)5u[(fo)-6.2(000.0.4(o

The **area** parameter limits the display to a specific configuration area. (For more information, see the )

The **all** parameter includes all commands that are set at the default value. Without the **all** parameter, the **show config** command lists only those configuration commands set to a value other than the default parameter.

To display the running configuration, type the following command:

```
MX# show config
# Configuration nvgen'd at 2007-5-10 19:08:38
# Image 2.1.0
# Model MX
# Last change occurred at 2007-5-10 16:31:14
set trace authentication level 10
set ip dns server 10.10.10.69 PRIMARY
set ip dns server 10.20.10.69 SECONDARY
set ip route default 10.8.1.1 1
set log console disable severity debug
set log session disable severity alert
set log buffer enable severity error messages 200
set log trace disable severity error mbytes 10
set log server 192.168.253.11 severity critical
set timezone PS  -8 0
set summertime PD  start first sun apr 2 0 end last sun oct 2 0
set system name MX
set system countrycode  S
set system contact trapeze-pubs
set radius server r1 address 192.168.253.1 key sunflower
set server group sg1 members r1
set enablepass password b6b706525e1814394621eeb2a1c4d5803fcf
set authentication console * none
set authentication admin * none
set user tech password encrypted 1315021018
press any key to continue, q to quit.
```

To display only the VLAN configuration commands, type the following command:

```
MX# show config area vlan
# Configuration nvgen'd at 2004-5-10 19:08:38
# Image 2.1.0
# Model MX
# Last change occurred at 2004-5-10 16:31:14
set vlan 1 port 1
set vlan 10 name backbone tunnel-affinity 5
set vlan 10 port 21
set vlan 10 port 22
set vlan 3 name red tunnel-affinity 5
set igmp mrsol mrsi 60 vlan 1
set igmp mrsol mrsi 60 vlan 10
```

## Saving Configuration Changes

To save the current configuration to a configuration file, use the following command:

```
save config [filename]
```

If you do not specify a filename of up to 128 alphanumeric characters, the command replaces the startup configuration file that was loaded the last time the software was rebooted. (To display the filename of that configuration file, see **"Displaying Boot Information" on page 3–2**.)

To save the running configuration to the file loaded the last time the software was rebooted, type the following command:

```
MX# save config
success: configuration saved.
```

To save the running configuration to a file named , type the following command:

```
MX# save config newconfig
```

```
success: configuration saved to newconfig.
```

## Specifying the Configuration File to Use After the Next Reboot

By default, the MX loads the configuration file named following a software reboot. To use a different configuration file after rebooting, use the following command:

```
set boot configuration-file filename
```

To configure an MX to load the configuration file following the next software reboot, type the following command:

```
MX# set boot configuration-file floor2mx
success: boot config set.
```

## Loading a Configuration File


This command completely re

To load configuration commands from a file into the MX current configuration, use the following command:

```
load config [url]
```

The default URL is the name of the configuration file loaded after the last reboot.

To load a configuration file named , type the following command:

```
MX# load config newconfig
Reloading configuration may result in lost of connectivity, do you wish to continue?
         (y/n) [n]y
success: Configuration reloaded
```

After you type **y**, MSS replaces the current configuration with the configuration in the file. If you type **n**, MSS does not load the file and the current configuration remains unchanged.

## Specifying a Backup Configuration File

In the event that part of the configuration file is invalid or otherwise unreadable, MSS does not load the file. You can optionally specify a backup file to load if MSS cannot load the original configuration file.

To specify a backup configuration file, use the following command:

```
set boot backup-configuration filename
```

To specify a file called as the backup configuration file, use the following command:

```
MX# set boot backup-configuration backup.cfg
success: backup boot config filename set.
```

After enabling this feature, you can clear a backup configuration file by entering the following command:

```
MX# clear boot backup-config
success: Backup boot config filename was cleared.
```

To display the name of the file specified as the backup configuration file, enter the **show boot** command. For example:

```
pubs# show boot
Configured boot version:         6.1.0.60
Configured boot image:           boot0:mx060t09.020
Configured boot configuration:   file:configuration
Backup boot configuration:       backup.cfg
Booted version:                  6.1.0.60
Booted image:                    boot0:mx060t09.020
Booted configuration:            file:configuration
Product model:                   MX
```

### Resetting to the Factory Default Configuration

To reset the MX to a factory default configuration, use the following command:

```
clear boot config
```

This command removes the configuration file used when the MX is rebooted.

To back up the current configuration file named and reset the MX to the factory default configuration, type the following commands:

```
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 ......
```

The **reset system force** command reboots the MX. The **force** option immediately restarts the system and reboots. If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the files do not match, the MX does not restart but instead displays a message advising you to either save the configuration changes or use the **force** option.

## Backing Up and Restoring the System

The following commands enable you to easily backup and restore MX system and user files:

```
backup system [tftp:/ip-addr/]filename [all | critical]
restore system [tftp:/ip-addr/]filename [all | critical] [force]
```

The **backup** command creates an archive in Unix ( ) format.

The **restore** command unzips an archive created by the **backup** command and copies the files from the archive onto the MX. If a file in the archive is duplicated on the MX, the archive version of the file replaces the file on the MX. The **restore** command does not delete files without duplicates 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.

You can create or unzip an archive located on a TFTP server or on the MX. If you specify a TFTP server as part of the filename with the **backup** command, the archive is copied directly to the TFTP server and not stored locally on the MX.

Both commands have options to specify the types of files to back up and restore:

- **critical**—Backs up or restores system files, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less. This is the default for the **restore** command.

## Backup and Restore 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 address, so the archive is not stored locally on the MX.

```
MX# backup system tftp:/10.10.20.9/sysa_bak critical

success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

### Displaying and Clearing an Administrative Console Session

To view information about the user with administrative access to the MX through a console plugged into the switch, type the following command:

```
MX# show sessions console
Tty         Username              Time (s)    Type
-------     --------------------  --------    ----
tty0                              5310        Console

1 console session
```

To clear the administrative sessions of a console user, type the following command:

```
MX# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [y]y
```

### Displaying and Clearing Administrative Telnet Sessions

To view information about administrative Telnet sessions, type the following command:

```
MX# show sessions telnet client
Tty         Username              Time (s)    Type
-------     --------------------  --------    ----
tty3        sshadmin              2099        SSH

1 telnet session
```

To clear the administrative sessions of Telnet users, type the following command:

```
MX# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [y]y
```

### Displaying and Clearing Client Telnet Sessions

To view administrative sessions of Telnet clients, type the following command:

```
MX# show sessions telnet client
Session   Server Address    Server Port    Client Port
-------   --------------    ------------   -----------
0          192.168.1.81     23             48000
1           10.10.1.22      23             48001
```

To clear the administrative sessions of Telnet clients, use the following command:

**clear sessions telnet** [**client** [*session-id*]]

You can clear all Telnet client sessions or a particular session. For example, the following command clears Telnet client session 1:

```
MX# clear sessions telnet client 1
```

## Displaying and Clearing Network Sessions

Use the following command to display information about network sessions:

```
Tx peak A-MSDU              0             0
Tx peak A-MPDU              0             0
Queue       Tx Packets  Tx Dropped  Re-Transmit  Rx Dropped
----------  ----------  ----------  -----------  ----------
Background           0           0            0           0
BestEffort           0           0            0           0
Video                0           0            0           0
Voice                0           0            0           0
```

## Displaying and Clearing Network Sessions by Username

You can view sessions by a username or user glob.

To see all sessions for a specific user or for a group of users, type the following command:

**show sessions network user** *user-glob*

For example, the following command shows all sessions of users whose names begin with :

```
MX# show sessions network user E*
User                            Sess  IP or MAC         VLAN            Port/
Name                              ID  Address           Name            Radio
------------------------------ ----  ----------------- --------------
EXAMPLE\singh                 12* 192.168.12.185    vlan-eng         3/2
EXAMPLE\havel                 13* 192.168.12.104    vlan-eng         1/2

2 sessions match criteria (of 3 total)
```

Use the **verbose** keyword to see more information. For example, the following command displays detailed session information about nin@example.com:

```
MX# show sessions network user nin@example.com verbose
User                            Sess  IP or MAC         VLAN            Port/
Name                              ID  Address           Name            Radio
------------------------------ ----  ----------------- --------------- -----
nin@example.com                   5* 192.168.12.141    vlan-eng         1/1
Client MAC: 00:02:2d:6e:ab:a5   GID: SESS-5-000430-686792-d8b3c564
State: ACTIVE                  (prev AUTHORIZED)
now on: MX 192.168.12.7, port 1, AP/radio 0422900147/1, as of 00:23:32 ago

1 sessions match criteria (of 10 total)
```

To clear all the network sessions of a user or group of users, use the following command:

**clear sessions network user** *user-glob*

For example, the following command clears the sessions of users named Bob:

```
MX-20# clear sessions network user Bob*
```

## Displaying and Clearing Network Sessions by MAC Address

You can view sessions by MAC address or MAC address glob. To view session information for a MAC address or set of MAC addresses, type the following command:

**show sessions network mac-addr** *mac-addr-glob*

For example, the following command displays the sessions for MAC address 01:05:5d:7e:98:1a:

```
MX# show sessions net mac-addr 01:05:5d:7e:98:1a
User                            Sess  IP or MAC         VLAN            Port/
Name                              ID  Address           Name            Radio
```

```
-------------------------- ----  -------------- ------------ -----
EXAMPLE\havel               13* 192.168.12.104   vlan-eng         1/2
```

To clear all the network sessions for a MAC address or set of MAC addresses, use the following command:

**clear sessions network mac-addr** *mac-addr-glob*

For example, to clear all sessions for MAC address 00:01:02:04:05:06, type the following command:

```
MX-20# clear sessions network mac-addr 00:01:02:04:05:06
```

## Displaying and Clearing Network Sessions by VLAN Name

You can view all session information for a specific VLAN or VLAN glob.

To see all network sessions information for a VLAN or set of VLANs, type the following command:

**show sessions network vlan** *vlan-glob*

For example, the following command displays the sessions for VLAN :

```
MX# show sessions network vlan west
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
EXAMPLE\tamara                 8* 192.168.12.174     west              1/1
host/laptop.example.com       11* 192.168.12.164     west              2/1
EXAMPLE\havel                 17* 192.168.12.195     west              1/2
EXAMPLE\jose                  20* 192.168.12.171     west              1/2
EXAMPLE\geetha                21* 192.168.12.169     west              3/2
```

To clear the sessions on a VLAN or set of VLANs, use the following command:

**clear sessions network vlan** *vlan-glob*

For example, the following command clears the sessions of all users on VLAN :

```
MX# clear sessions network vlan red
```

## Displaying and Clearing Network Sessions by Session ID

You can display information about a session by session ID. To find local session IDs, enter the **show sessions** command. You can view more detailed information for an individual session, including authorization parameters and, for wireless sessions, packet and radio statistics.

For example, to display information about session 27, type the following command:

```
MX# show sessions network session-id 88
Local Id:    88
Global Id:   SESS-88-00040f-876766-623fd6
State:       ACTIVE
SSID:        Rack-39-PM
Port/Radio:  10/1
MAC Address: 00:0f:66:f4:71:6d
User Name:   last-resort-Rack-39-PM
IP Address:  10.2.39.217
Vlan Name:   default
Tag:         1
Session Start:   Wed Apr 12 21:19:27 2006 GMT
Last Auth Time:  Wed Apr 12 21:19:26 2006 GMT
Last Activity:   Wed Apr 12 21:19:49 2006 GMT  ( <15s ago)
Session Timeout: 0
Idle Time-To-Live: 175
Login Type:      LAST-RESORT
EAP Method:      NONE, using server 172.16.0.1
Session statistics as updated from AP:
```

For example, to change the user idle timeout for service profile to 6 minutes (360 seconds), use the following command:

```
MX# set service-profile sp1 user-idle-timeout 360
success: change accepted.
```

To disable the user idle timeout, use the following command:

```
MX# set service-profile sp1 user-idle-timeout 0
success: change accepted.
```

5

# Enabling and Logging Into WebView

WebView is a Web-based management application available on MX switches. You can use WebView for common configuration and management tasks. On most MX models (MX-200, MX-216, MX-8, or MXR-2), you also can use WebView to perform initial configuration of a new MX.

## System Requirements

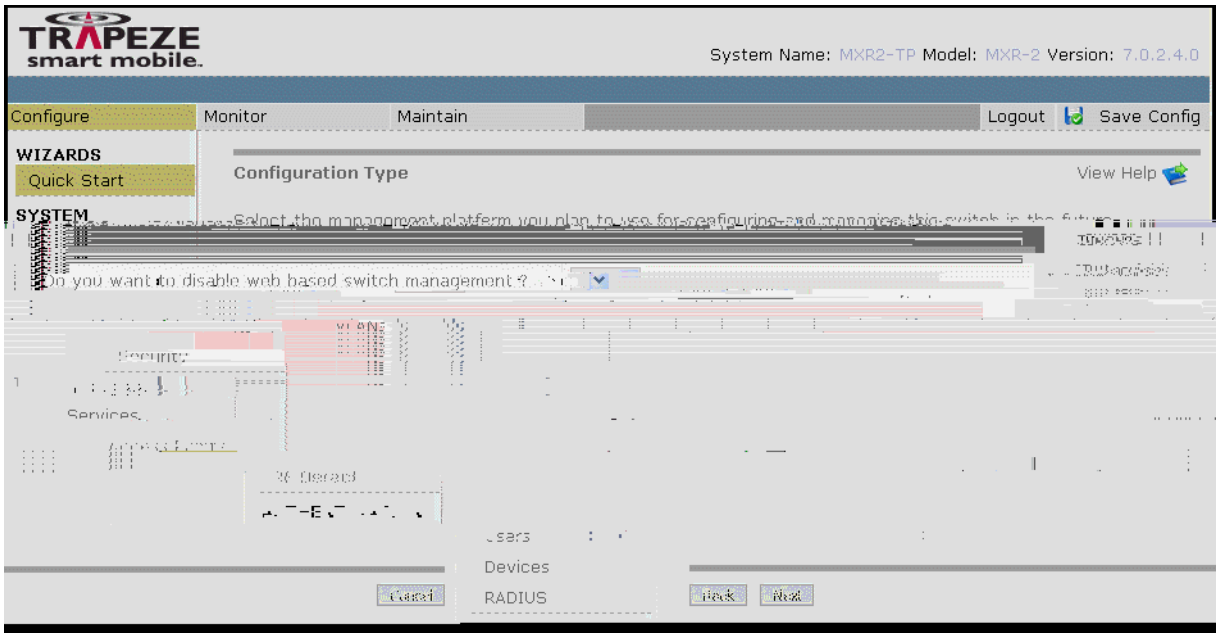
### Browser Requirements

WebView is supported on the following browsers:

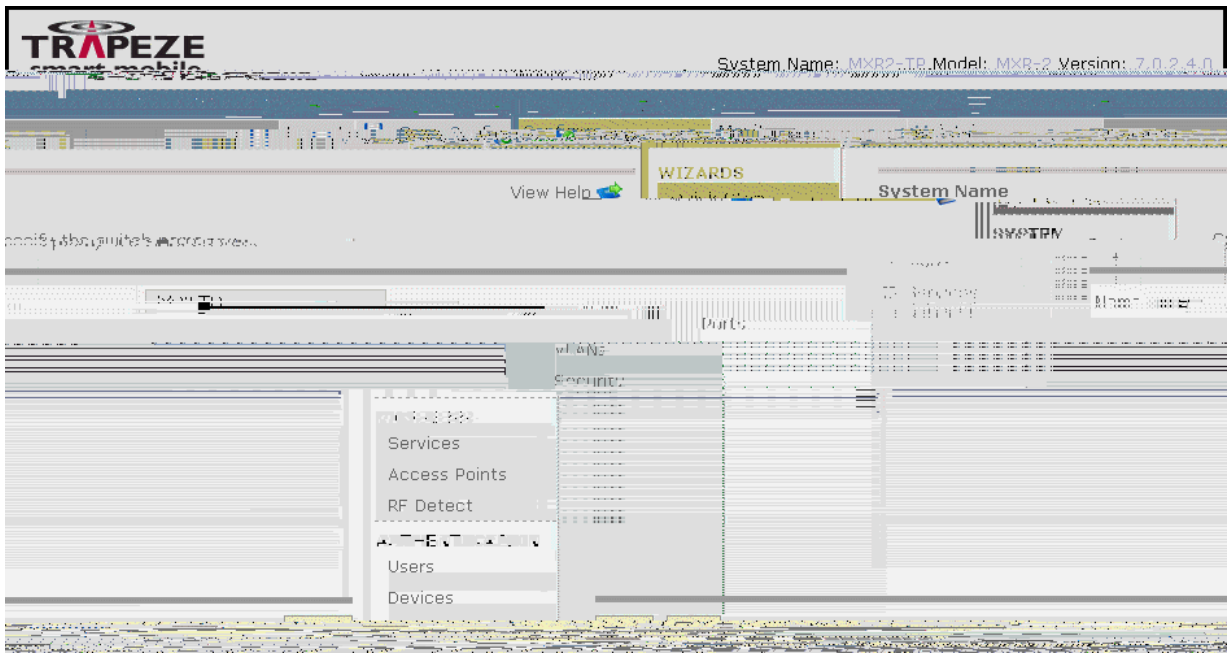
- Mozilla Firefox Version 1.0 or later
- Microsoft Internet Explorer Version 6.0 or later

TLS 1.0, SSL 2.0, or SSL 3.0 must be enabled in the browser. To enable TLS 1.0, SSL 2.0, or SSL

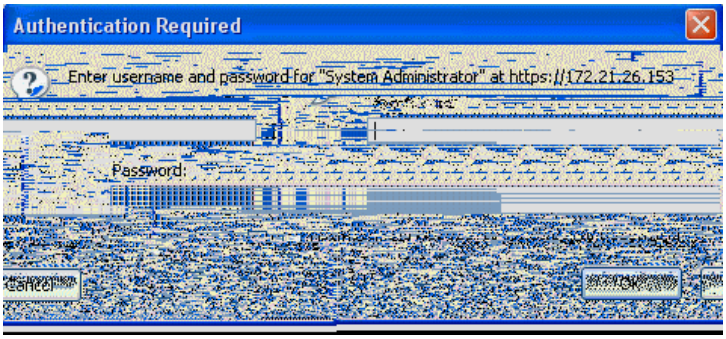
3. If you plan to continue using WebView to manage the MX, select **No** to keep WebView enabled on the MX. Click **Next**.



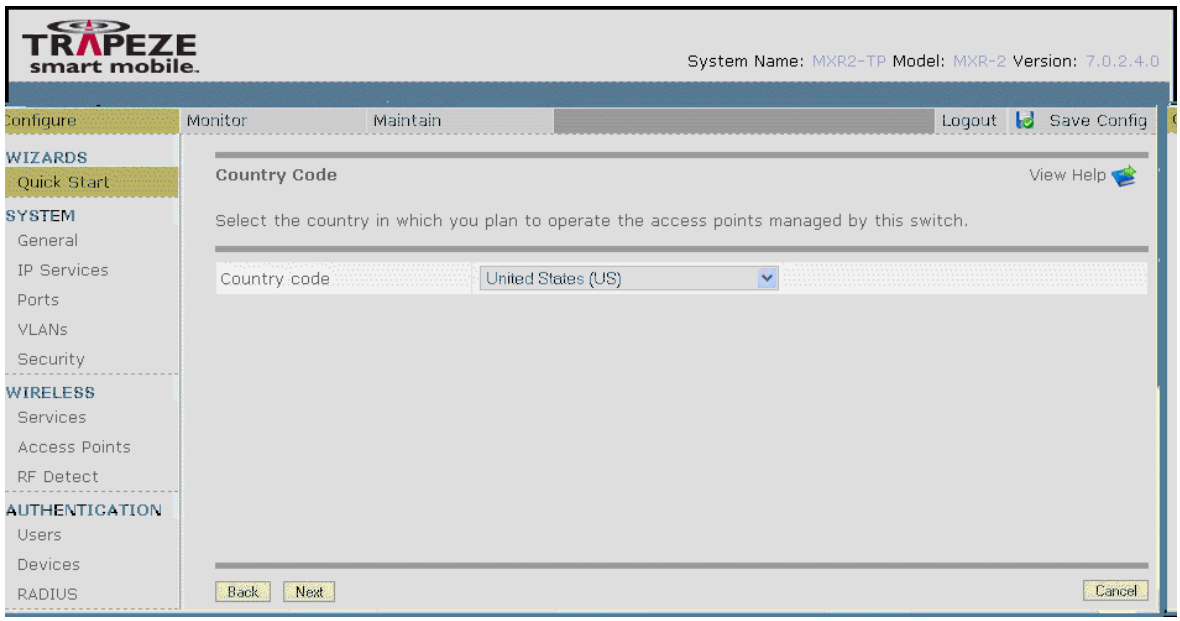

4. In the **Name** field, type the name for the MX and click **Next**.



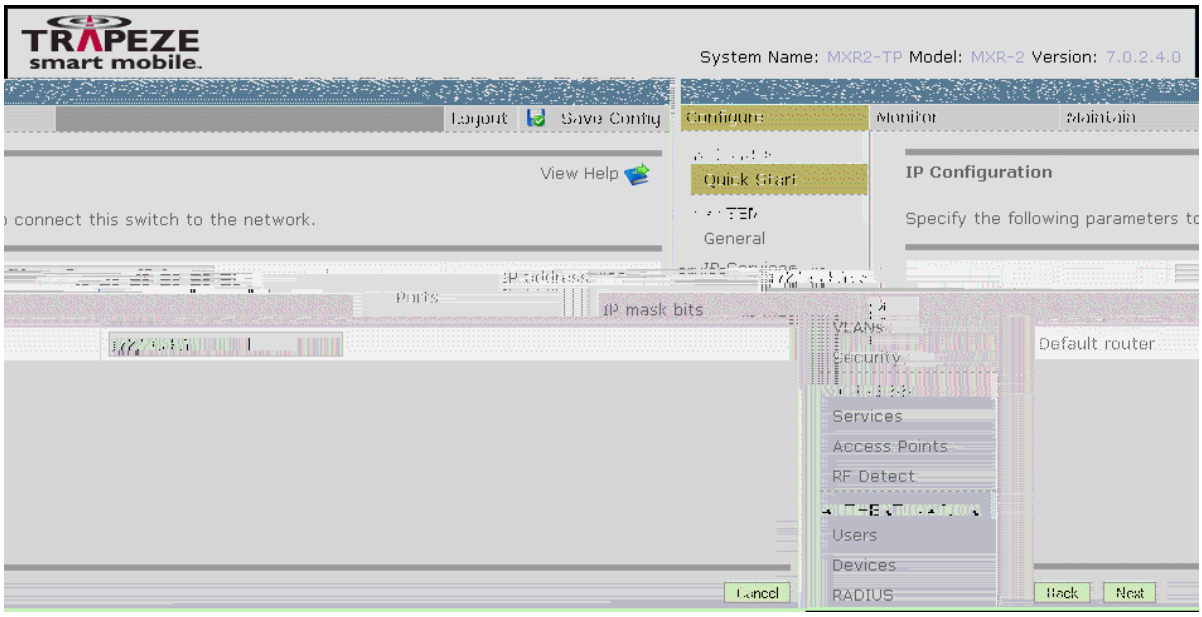
5. The **Authentication Required** dialogue box is displayed. Type your **User Name** and **Password** and click **OK**.



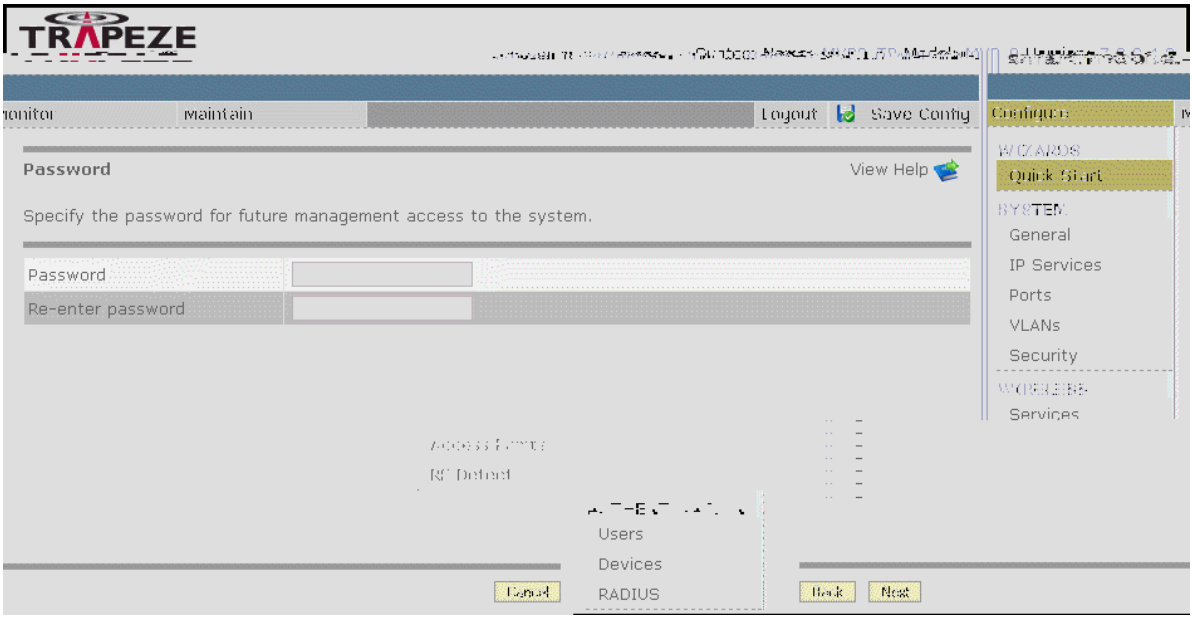

6. Select the country code for your location from the **Country code** list and click **Next**.



7. In the **IP address**, **IP mask bits**, and **Default router** fields, type your specific MX information and click **Next**.




8. In the **Password** and **Re-enter password** fields, type and re-type your password. This password allows you to access the system in the future. Click **Next**.

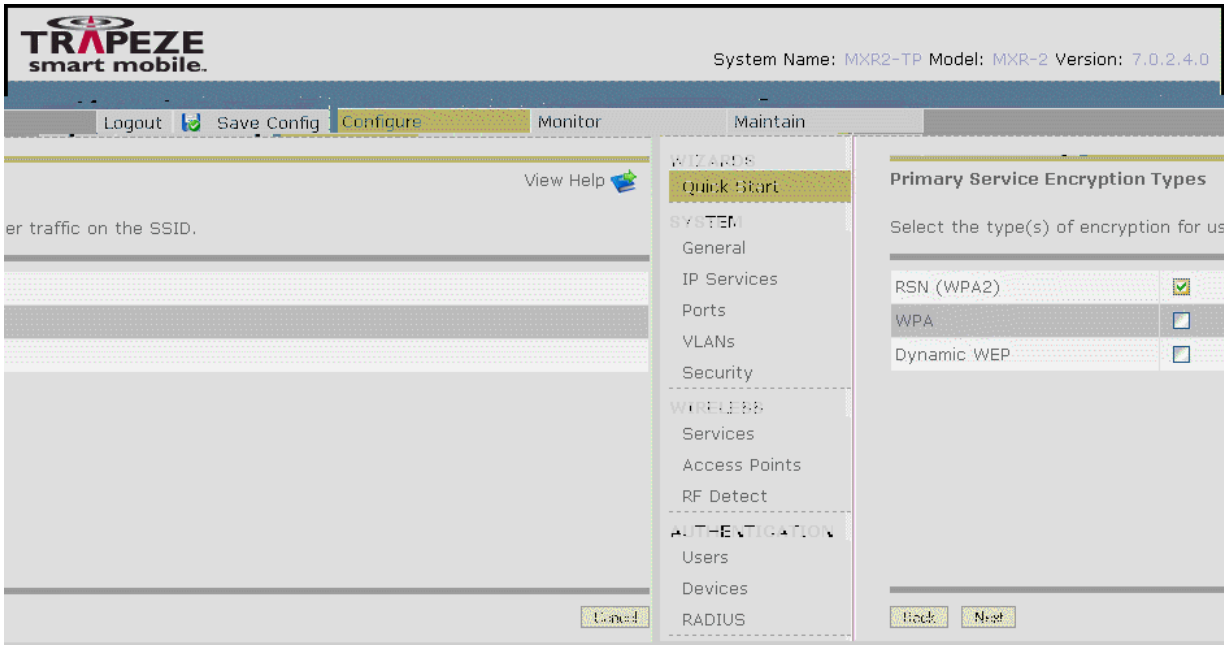


9. To set the date and time of the MX, type the **Date** and **Time**, select a Time zone from the **Time zone** list, and select options to **Enable NTP** or **Enable Daylight Savings Time**, if needed. Click **Next.**

10. In the **DST Name** field, type a name for your Daylight Savings Time zone and set the

**13.** Select **Yes** to add tags to the default VLAN. The default value is **No**. Click **Next**.

**14.** Select the **desired level of encryption for user traffic on the SSID**. Click **Next**.

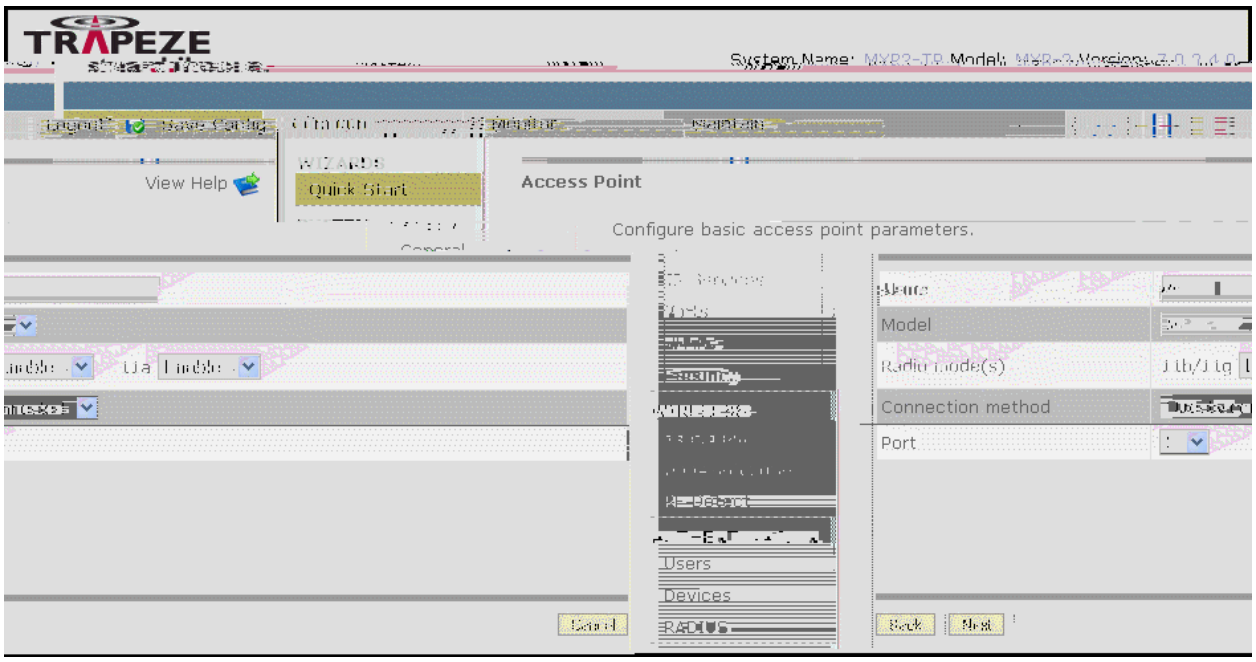


**15.** Select the desired encryption algorithms for user traffic on the network. Click **Next**.

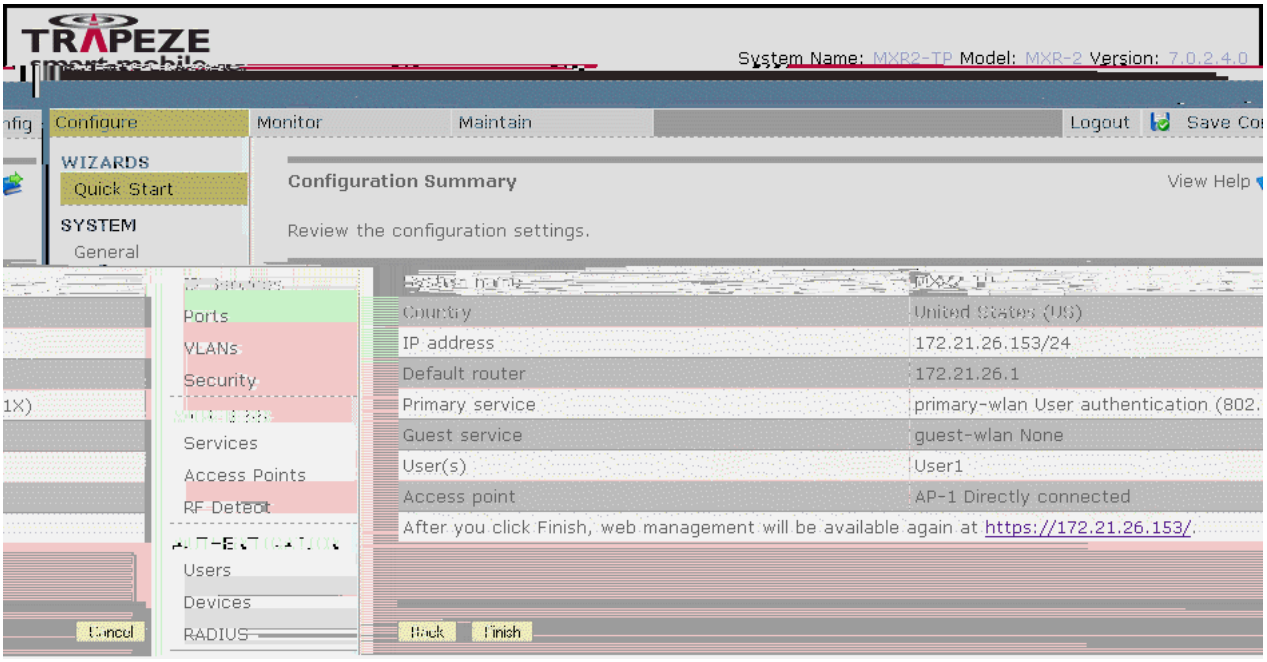
**16.** Select either **Local user database** or **Retabit**

17. Create one or more local users to be stored in the MX's local user database on the MX. For each user, type in a user **Name**

**19.** Use this **Access Point** page to configure your basic access point parameters. In the **Name** field, type a name for your access point, select a **Model** type from the **Model** list, and select **Enable** to activate each radio mode from the **Radio mode(s)** list. Select a **Connection method** and a **Port** number from the lists. Click **Next**.




**20.** Review your configuration settings on the **Configuration Summary** page and click **Finish**. You also have the option to use the **Back** button to correct configuration errors.



6

# Configuring  Administrative and Local Access

# First-Time Configuration via the Console

Administrators must initially configure the MX with a computer or terminal connected to the MX console port through a serial cable. Telnet access is not initially enabled.

To configure a previously unconfigured MX through the console, you must complete the following tasks:

3. At the “Enter new password” prompt, enter an enable password of up to 32 alphanumeric characters with no spaces. The password is not displayed as you type it.

4. Type the password again to confirm it.

   The password is now set.

```
MX# set enablepass
Enter old password:
Enter new password:
Retype new password:
Password changed
```

5. Store the configuration by typing the following command:

```
MX# save config
success: configuration saved.
```

## ingMaster Enable Password

ou use RingMaster to continue configuring the MX, enter the enable password of the MX when
upload the MX configuration into RingMaster. (For RingMaster information, see the

## )Authenticating at the Console

You can configure the console to require authentication or not require authentication. Trapeze Networks recommends that you enforce authentication on the console port.

To enforce console authentication, take the following steps:

1. Add a user in the local database by typing the following command with a username and password:

```
MX# set user username password password
success: change accepted.
```

2. To enforce the use of console authentication via the local database, type the following command:

```
MX# set authentication console * local
```

3. To store this configuration into nonvolatile memory, type the following command:

```
MX# save config
success: configuration saved.
```

By default, no authentication is required at the console. If you previously required authentication and have decided not to require it (during testing, for example), type the following command to configure the console so that it does require username and password authentication:

```
MX# set authentication console * none
```


The authentication method **none** you can specify for administrative access is different f32k the fallthru authentication type None, which applies only to network access. The authentication method none allows access to the MX by an administrator. The fallthru authentication type None denies access to a network user. (For information about the fallthru authentication types, see **"Authentication Algorithm" on page 11–2**.)

# Passwords Overview

Trapeze Networks recommends that all users create passwords that are memorable to themselves, difficult for others to guess, and not subject to a dictionary attack.

By default, user passwords are automatically encrypted when entered in the local database. However, the encryption is not strong. To maintain security, MSS displays only the encrypted form of the password in **show** commands.

Optionally, you can configure MSS so that the following additional restrictions apply to user passwords:

- Passwords must be a minimum of 10 characters in length, and a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each (for example, ).
- A user cannot reuse any of the 10 previous passwords (not applicable to network users).
- When a user changes his or her password, at least 4 characters must be different f32k the previous password.
- A user password expires after a configured amount of time.
- A user is locked out of the system after a configured number of failed login attempts. When this happens, a trap is generated and an alert is logged. (Administrative users can gain access to the system through the console even when the account is locked.)
- Only one unsuccessful login attempt is allowed in a 10-second period for a user or session.
- All administrative logins, logouts, logouts due to idle timeout, and disconnects are logged.
- The audit log file on the MX ( ) cannot be deleted, and attempts to delete log files are recorded.

These restrictions are disabled by default.

## Configuring Passwords

This section describes the following tasks:

- Setting a password for a user in the local database.
- Enabling restrictions on password usage.
- Setting the maximum number of failed login attempts for a user.
- Specifying the minimum allowable password length.
- Setting the length of time before password expiration.
- Restoring access to a user locked out of the system.

### Setting Passwords for Local Users

To configure a user password in the local database, type the following command:

```
set user username password [encrypted] password
```

For example, to configure user Jose with the password in the local database on the MX, type the following command:

```
MX# set user Jose password spRin9
success:  ser Jose created
```

The **encrypted** option indicates that the password string you are entering is the encrypted form of the password. Use this option only if you do not want MSS to encrypt the password for you.

## Specifying Minimum Password Length

To specify the minimum allowable length for user passwords, use the following command:

```
set authentication minimum-password-length length
```

You can specify a minimum password length between 0 – 32 characters. Specifying 0 removes the restriction on password length. By default, there is no 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 and displays a list of users with passwords that do not meet the minimum length restriction.

For example, 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 pass-
         word length -
 dan
 admin
 user2
 jdoe
success: change accepted.
```

## Configuring Password Expiration Time

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

```
MX# clear user Nin lockout
```

# Configuring and Managing Ports and VLANs

## Configuring and Managing Ports

You can configure and display information for the following port parameters:

- Port type
- Name
- Speed and autonegotiation
- Port state
- Power over Ethernet (PoE) state
- Load sharing

### Setting the Port Type

An MX port can be one of the following types:

- Network port — A network port is a Layer 2 switch port connecting the MX to other networking devices such as switches and routers.
- MP port — An MP connects the MX to an MP. The port also can provide power to the MP. Wireless users are authenticated on the network through an MP port.


A Distributed MP, which is connected to MX switches through intermediate Layer 2 or Layer 3 networks, does not use an MP access port. To configure for a Distributed MP, see **"Configuring an MP Connection" on page 7–3** and Chapter , "Configuring Mobility Points," on page 1.

- Wired authentication port — A wired authentication port connects the MX to user devices, such as workstations, that must authenticate in order to access the network.

All MX ports are network ports by default. You must set the port type for ports directly connected to MPs and for ports on wired user stations that must authenticate in order to access the network. When you change port type, MSS applies default settings appropriate for the port type. **Table 7–1** lists the default settings applied for each port type. For example, the MP column lists default settings that MSS applies when you change a port type to **ap** (an MP access point).

**Table 7– 1. Port Defaults Set By Port Type Change**

| Parameter | Port type | | |
|---|---|---|---|
| | MP Access | Wired Authentication | Network |
| VLAN membership | | | |

but can be configured for 802.11b or 802.11g exclusively. If the country of operation specified by the **set system countrycode** command does not allow 802.11g, the default is 802.11b.


Models MP-52, MP-241, MP-252, MP-262, MP-341, and MP-352 have been discontinued but are still supported by the command.


The radios for an MP-620 require external antennas, and model MP-262 requires an external antenna for the 802.11b/g radio. The following models have internal antennas but also have connectors for optional use of external antennas: MP-372, MP-372-JP, AP3750, AP3850, 2330, and 2330A. (Antenna support on a specific model is limited to the antennas certified for use with that model.) To specify the antenna model, use the **set ap** < > **radio** < > **antennatype** command. (See **"Configuring the External Antenna Model and Location" on page 12–38**.)

To set ports 4 through 6 for an MP-372 and enable PoE on the ports, type the following command:

```
MX# set ap 4-6 port 1 model mp-372 poe enable
 his may affect the power applied on the configured ports. Would you like to con-
         tinue?
         (y/n) [n]y
success: change accepted.
```

## Configuring an MP Connection

To configure a connection for an MP (referred to as an in the CLI), use the following command:

```
set ap  serial-id serial-ID
         model {2330 | 2330A | 2330B | 2332-A1 | AP2750 | AP3750 | AP3850 | AP1602 ||
         AP1602C| AP3950 | mp-371 | mp-372A | mp-372 | mp-372-JP | mp-422 |mp-422A |
         Mp-422F | | mp-432 | mp-620 | mp-620A } [radiotype {11a | 11b| 11g}]
```

The variable refers to an index value that identifies the MP on the MX. This value is not related to the port connected to the MP.

For the **serial-id** parameter, specify the serial number of the MP. The serial number is listed on the MP case. To display the serial number using the CLI, use the **show version details** command.

To configure a connection for MP 1, which is an MP model MP-372 with serial-ID 0322199999, type the following command:

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

## Setting a Port for a Wired Authentication User

To set a port for a wired authentication user, use the following command:

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

You must specify a port list. Optionally, you also can specify a tag-list to subdivide the port into virtual ports, set the maximum number of simultaneous user sessions that can be active on the port, and change the fallthru authentication type.

By default, one user session can be active on the port at a time.

The authentication type is used if the user does not support 802.1X and is not authenticated by MAC authentication. The default is none, and the user is automatically denied access if neither 802.1X authentication or MAC authentication is successful.

To set port 17 as a wired authentication port, type the following command:

```
MX# set port type wired-auth 17
success: change accepted
```

This command configures port 17 as a wired authentication port supporting one interface and one simultaneous user session.

For 802.1X clients, wired authentication works if the clients are directly attached to the wired authentication port, or are attached through a hub that does not block forwarding of packets from the client to the PAE group address (01:80:c2:00:00:03). Wired authentication works in accordance with the 802.1X specification, which prohibits a client from sending traffic directly to an authenticator MAC address until the client is authenticated, because it is possible for multiple authenticators to acquire the same client. Instead of sending traffic to the authenticator MAC address, the client sends packets to the PAE group address.

For non-802.1X clients, who use MAC authentication, WebAAA, or last-resort authentication,


A cleared port is not placed in any VLANs, not even the default VLAN (VLAN 1).

To clear a port, use the following command:

```
clear port type port-list
```

For example, to clear the port settings from port 5 and reset the port as a network port, type the following command:

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

### Clearing a Distributed MP

To clear a Distributed MP, use the following command:

```
clear ap
```

## Configuring a Port Name

Each MX port has a number but does not have a name by default.

### Setting a Port Name

To set a port name, use the following command:

```
set port port name name
```

You can specify only a single port number with the command.

To set the name of port 17 to , type the following command:

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

### Removing a Port Name

To remove a port name, use the following command:

```
clear port port-list name
```

## Configuring Media Type on a Dual-Interface Gigabit Ethernet Port

The gigabit Ethernet ports on an MX-400 have two physical interfaces: a 1000BASE-TX copper interface and a 1000BASE-SX or 1000BASE-LX fiber interface. The copper interface is provided by a built-in RJ-45 connector. The fiber interface is optional and requires insertion of a Gigabit interface converter (GBIC).

Only one interface can be active on a port. By default, the GBIC (fiber) interface is active. You can configure a port to use the RJ-45 (copper) interface instead.

If you set the port interface to RJ-45 on a port with an active fiber link, MSS immediately changes the link to the copper interface.

To disable the fiber interface and enable the copper interface on an MX-400 port, use the following command:

```
set port media-type port-list rj45
```

To disable the copper interface and reenable the fiber interface on an MX-400 port, use the following command:

```
clear port media-type port-list
```

To display the enabled interface type for each port, use the following command:

```
show port media-type [port-list]
```

To disable the fiber interface and enable the copper interface of port 2 on an MX-400 and verify the change, type the following commands:

```
MX-400# set port media-type 2 rj45
MX-400# show port media-type
Port  Media  ype
============================================================
   1  GBIC
   2  RJ45
   3  GBIC
   4  GBIC
```

## Configuring Port Operating Parameters

Autonegotiation is enabled by default on an MX 10/100 Ethernet ports and gigabit Ethernet ports.


You can configure the following port operating parameters:

- Speed
- Autonegotiation
- Port state
- PoE state

You also can set the administrative state of a port and PoE setting to off and then back on to reset the port.

### 10/100 Ports—Autonegotiation and Port Speed

MX 10/100 Ethernet ports use autonegotiation by default to determine the appropriate port speed.

To explicitly set the port speed of a 10/100 port, use the following command:

```
set port speed port-list {10 | 100 | auto}
```

To set the port speed on ports 1, 7 through 11, and 14 to 10 Mbps, type the following command:

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

## Gigabit Ports—Autonegotiation and Flow Control

By default, MX gigabit ports use autonegotiation to determine capabilities for 802.3z flow control parameters. The gigabit ports can respond to IEEE 802.3z flow control packets. Some devices use this capability to prevent packet loss by temporarily pausing data transmission.

## Disabling a Port

All ports are enabled by default. To administratively disable a port, use the following command:

```
set port {enable | disable} port-list
```

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

## Disabling Power over Ethernet

Power over Ethernet (PoE) supplies DC power to a device connected to an MP. The PoE state depends on whether you enable or disable PoE when you set the port type. (See **"Setting the Port Type" on page 7–1**.)

To change the PoE state on a port, use the following command:

```
set port poe port-list enable | disable
```

## Displaying Port Information

You can use CLI commands to display the following port information:

- Port configuration and status
- PoE state
- Port statistics

You also can configure MSS to display and regularly update port statistics in a separate window.

### Displaying Port Configuration and Status

To display port configuration and status information, use the following command:

```
show port status [port-list]
```

To display information for all ports, type the following command:

```
MX# show port status
Port  Name            Admin  Oper   Config     Actual    ype        Media
================================================================================
   1  1               up     up       auto      100/full  network    10/100Base x
   2  2               up     down     auto                network    10/100Base x
   3  3               up     down     auto                network    10/100Base x
   4  4               up     down     auto                network    10/100Base x
   5  5               up     down     auto                network    10/100Base x
   6  6               up     down     auto                network    10/100Base x
   7  7               up     down     auto                network    10/100Base x
   8  8               up     down     auto                network    10/100Base x
   9  9               up     up       auto      100/full  ap         10/100Base x
  10  10              up     up       auto      100/full  network    10/100Base x
  11  11              up     down     auto                network    10/100Base x
  12  12              up     down     auto                network    10/100Base x
  13  13              up     down     auto                network    10/100Base x
  14  14              up     down     auto                network    10/100Base x
  15  15              up     down     auto                network    10/100Base x
  16  16              up     down     auto                network    10/100Base x
  17  17              up     down     auto                network    10/100Base x
  18  18              up     down     auto                network    10/100Base x
  19  19              up     down     auto                network    10/100Base x
  20  20              up     down     auto                network    10/100Base x
  21  21              up     down     auto                network    no connector
  22  22              up     down     auto                network    no connector
```

In this example, three of the MX ports, 1, 9, and 10, have an operational status of , indicating the links on the ports are available. Ports 1 and 10 are network ports. Port 9 is an MP.

(For more information about the fields in the output, see the )

### Displaying PoE State

To display the PoE state of a port, use the following command:

```
show port poe [port-list]
```

To display PoE information for ports 7 and 9, type the following command:

```
MX# show port poe 7,9
              Link     Port    PoE       PoE
Port  Name           Status    ype    config    Draw
================================================================================
   7  7               down     MP     disabled  off
   9  9               up       MP     enabled   1.44
```

In this example, PoE is disabled on port 7 and enabled on port 9. The MP connected to port 9 is drawing 1.44 W of power from the MX .

(For more information about the fields in the output, see the .)

## Displaying Port Statistics

To display port statistics, use the following command:

```
show port counters [octets | packets | receive-errors | transmit-errors | collisions
        | receive-etherstats | transmit-etherstats] [port port-list]
```

You can specify one statistic type with the command. For example, to display octet statistics for port 3, type the following command:

```
MX# show port counters octets port 3
Port   Status                      Rx Octets                          x Octets
================================================================================
    3   p                         27965420                         34886544
```

(For information about the fields in the output, see the
.)

## Clearing Statistics Counters

To clear all port statistics counters, use the following command:

```
clear port counters
```

The counters begin incrementing again, starting from 0.

## Monitoring Port Statistics

You can display port statistics in a format that continually updates the counters. When you enable monitoring of port statistics, MSS clears the CLI session window and displays the statistics at the top of the window. MSS refreshes the statistics every 5 seconds. This interval cannot be configured.

To monitor port statistics, use the following command:

```
monitor port counters [octets | packets | receive-errors | transmit-errors | colli-
        sions | receive-etherstats | transmit-etherstats]
```

Statistics types are displayed in the following order by default:

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

Each type of statistic is displayed separately. Press the Spacebar on your keyboard to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in

To monitor port statistics beginning with octet statistics (the defaul

Enter a name for the group and the ports contained in the group.

The **mode** parameter adds or removes ports for a previously configured group. To modify a group:

- Add ports—Enter the ports to add, then enter **mode on**.
- Remove ports—Enter the ports to remove, then enter **mode off**.

To configure a port group named containing ports 1 through 5 and enable the link, type the following command:

```
MX# set port-group name server1 1-5 mode on
success: change accepted.
```

After you configure a port group, you can use the port group name with commands that change Layer 2 configuration parameters and apply configuration changes to all ports in the port group. For example, Spanning Tree Protocol (STP) and VLAN membership changes affect the entire port group instead of individual ports. When you make Layer 2 configuration changes, you can use a port group name in place of the port list. Ethernet port statistics continue to apply to individual ports, not to port groups.

To configure a port group named containing ports 15 and 17 and add the ports to the VLAN, type the following commands:

```
MX# set port-group name server2 15,17 mode on
success: change accepted.
MX# set vlan default port server2
success: change accepted.
```

To verify the configuration change, type the following command:

```
MX# show vlan config
                     Admin  VLAN   unl                          Port
VLAN Name            Status State Affin Port              ag   State
---- ---------------- ------ ----- ----- ---------------- ----- -----
   1 default           p      p        5
                                         server2          none   p
```

To indicate that the ports are configured as a port group, the **show vlan config** output lists the port group name instead of the individual port numbers.

## Removing a Port Group

To remove a port group, use the following command:

```
clear port-group name name
```

## Displaying Port Group Information

To display port group information, use the following command:

```
show port-group [name group-name]
```

To display the configuration and status of port group , type the following command:

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

### Interoperating with Cisco Systems EtherChannel

Load-sharing port groups are interoperable with Cisco Systems EtherChannel capabilities. To configure a Cisco Catalyst to interoperate with a Trapeze Networks MX, use the following command on the Catalyst:

```
set port channel port-list mode on
```

# Configuring and Managing VLANs

## Understanding VLANs

A virtual LAN (VLAN) is a Layer 2 broadcast domain that can span multiple wired or wireless

- Tunnel-Private-Group-ID—This attribute is described in RFC 2868,
  .
- VLAN-Name—This attribute is a Trapeze vendor-specific attribute (VSA).

Specify the VLAN name, not the VLAN number. The examples in this chapter assume the VLAN is assigned on a RADIUS server with either of the valid attributes. (For more information, see Chapter , “Configuring AAA for Network Users,” on page 1.)

## VLAN Names

To create a VLAN, you must assign a name to it. VLAN names must be globally unique across a Mobility Domain to ensure the intended user connectivity as determined through authentication and authooJ-. -1.4036 TD6.0018 Tc-.0032 Tw[(VLAN-N)EveruniAN

If you use a tag value, Trapeze Networks recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same, but other vendors' devices may require it.


MSS automatically assigns tag values to Distributed MPs. Each of these tag values represents a unique combination of radio, encryption type, and VLAN. These tag values do not necessarily correspond to tag values configured on the VLAN ports connecting the Distributed MP to the MX.

### Tunnel Affinity

MXs configured as a Mobility Domain allow users to roam seamlessly across MPs and even across MXs. Although a MX that is not a member of a user VLAN cannot directly forward traffic for the user, the MX can tunnel the traffic to another MX that is a member of the user VLAN.

If the MX that is not in the user VLAN has a choice of more than one other MX to tunnel the user traffic, the MX selects the other MX based on an affinity value. This is a numeric value that each MX within a Mobility Domain advertises, for each of the VLANs, to all other switches in the Mobility Domain. An MX outside the user VLAN selects the other operational MX with the highest affinity value for the user VLAN to forward traffic for the user.

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

## Configuring a VLAN

You can configure the following VLAN parameters:

- VLAN number
- VLAN name
- Po4( fo)N5 list (the po4( fo)N5s in the VLAN)
- Per-poN5 tag value (an 802.1Q value representing a virtual poN5 in the VLAN)
- Tunnel affinity (a value that influences tunneling connections for roaming)
- MAC restriction list (if you want to prevent clien5s from communicating with one another directly at Layer 2)

### Creating a VLAN

To create a VLAN, use the following command:

`set vlan` *`vlan-num`* `name` *`name`*

Specify a VLAN number from 2 to 4093, and specify a name up to 16 alphabetic characters long.

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

You must assign a name to a VLAN before you can add poN5s to the VLAN. You can configure the name and add poN5s with a single **set vlan** command or separate **set vlan** commands.

Once you assign a VLAN number to a VLAN, you cannot change the number. However, you can change a VLAN name.

For example, to assign the name

To completely remove VLAN , type the following command:

```
MX# clear vlan ecru
 his may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```


## Changing Tunneling Affinity

To change the tunneling affinity, use the following command:

```
set vlan vlan-id tunnel-affinity num
```

Specify a value from 1 through 10. The default is 5.

## Restricting Layer 2 Forwarding Among Clients

By default, clients within a VLAN are able to communicate with one another directly at Layer 2. You can enhance network security by restricting Layer 2 forwarding among clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN default routers. Clients within the VLAN are not permitted to communicate directly. To communicate with another client, the client must use one of the specified default routers.

To restrict Layer 2 forwarding in a VLAN, use the following command:

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

You can specify multiple addresses by listing them on the same command line or by entering multiple commands.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the **mode enable** option with this command.

To change a MAC address, use the **clear security l2-restrict** command to remove it, then use the **set security l2-restrict** command to add the correct address.

```
clear security l2-restrict vlan vlan-id
         [permit-mac mac-addr [mac-addr] | all]
```

To display configuration information and statistics for Layer 2 forwarding restriction, use the following command:

```
show security l2-restrict [vlan vlan-id | all]
```

The following commands restrict Layer 2 forwarding of client data in VLAN to the default routers with MAC address aa:bb:cc:dd:ee:ff and 11:22:33:44:55:66, and display restriction information and statistics:

```
MX# set security l2-restrict vlan abc_air mode enable permit-mac aa:bb:cc:dd:ee:ff
         11:22:33:44:55:66
success: change accepted.
MX# show security l2-restrict
VLAN Name             En Drops      Permit MAC          Hits
---- ---------------- -- ---------- ------------------ ----------
   1 abc_air          Y           0 aa:bb:cc:dd:ee:ff         5947
                                    11:22:33:44:55:66            9
```

The En field indicates if restriction is enabled. The Drops field indicates how many packets were addressed directly from one client to another and dropped by MSS. The Hits field indicates how many packets the permitted default router has received from clients.

To reset the statistics counters, use the following command:

```
clear security l2-restrict counters [vlan vlan-id | all]
```

## Displaying VLAN Information

To display VLAN configuration information, use the following command:

```
show vlan config [vlan-id]
```

To display information for VLAN , type the following command:

```
MX# show vlan config burgundy
                      Admin  VLAN   unl                          Port
VLAN Name             Status State Affin Port               ag   State
---- ---------------- ------ ----- ----- ---------------- ----- -------- ----- --------0bt
                                          nvlan c
                                          nvlan c
```

To display all entries that begin with 00, type the following command:

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

(For information about the fields in the output, see the .)

## Adding an Entry to the Forwarding Database

To add an entry to the forwarding database, use the following command:

`set fdb {perm | static} mac-addr port port-list vlan vlan-id [tag tag-value]`

To add a permanent entry for MAC address 00:bb:cc:dd:ee:ff on ports 3 and 5 in VLAN , type the following command:

```
MX# set fdb perm 00:bb:cc:dd:ee:ff port 3,5 vlan blue
success: change accepted.
```

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

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

## Removing Entries from the Forwarding Database

To remove an entry from the forwarding database, use the following command:

`clear fdb {perm | static | dynamic | port port-list} [vlan vlan-id] [tag tag-value]`

To clear all dynamic forwarding database entries that match all VLANs, type the following command:

```
MX# clear fdb dynamic
success: change accepted.
```

To clear all dynamic forwarding database entries that match ports 3 and 5, type the following command:

```
MX# clear fdb port 3,5
success: change accepted.
```

## Configuring the Aging Timeout Period

The aging timeout period specifies how long a dynamic entry can remain unused before the software removes the entry from the database.

You can change the aging timeout period on an individual VLAN basis. You can change the timeout period to a value from 0 through 1,000,000 seconds. The default aging timeout period is 300 seconds (5 minutes). If you change the timeout period to 0, aging is disabled.

### Displaying the Aging Timeout Period

To display the current setting of the aging timeout period, use the following command:

`show fdb agingtime [vlan vlan-id]`

For example, to display the aging timeout period for all configured VLANs, type the following command:

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

### Changing the Aging Timeout Period

To change the aging timeout period, use the following command:

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

For example, to set the aging timeout period for VLAN 2 to 600 seconds, type the following command:

```
MX# set fdb agingtime 2 age 600
success: change accepted.
```

## Port and VLAN Configuration Scenario

This scenario assigns names to ports, and configures MP access ports, wired authentication ports, a load-sharing port group, and VLANs.

**1.** Assign names to ports to identify their functions, and verify the configuration change. Type the following commands:

```
MX# set port 1 name mx_mgmt
success: change accepted.
MX# set port 2 name finance
success: change accepted.
MX# set port 3 name accounting
success: change accepted.
MX# set port 4 name shipping
success: change accepted.
MX# set port 5 name lobby
success: change accepted.
MX# set port 6 name conf_room1
success: change accepted.
MX# set port 7 name conf_room2
success: change accepted.
MX# set port 8-13 name manufacturing
success: change accepted.
MX# set port 14-18 name rsrch_dev
success: change accepted.
MX# set port 19-20 name mobility
success: change accepted.
MX# set port 21,22 name backbone
success: change accepted.
MX# show port status
Port  Name            Admin  Oper    Config    Actual     ype       Media
================================================================================
   1  mx_mgmt         up     up      auto      100/full  network    10/100Base x
   2  finance         up     down    auto                network    10/100Base x
   3  accounting      up     down    auto                network    10/100Base x
   4  shipping        up     down    auto                network    10/100Base x
   5  lobby           up     down    auto                network    10/100Base x
   6  conf_room1      up     down    auto                network    10/100Base x
   7  conf_room2      up     down    auto                network    10/100Base x
   8  manufacturing   up     down    auto                network    10/100Base x
   9  manufacturing   up     down    auto                network    10/100Base x
  10  manufacturing   up     down    auto                network    10/100Base x
  11  manufacturing   up     down    auto                network    10/100Base x
  12  manufacturing   up     down    auto                network    10/100Base x
  13  manufacturing   up     down    auto                network    10/100Base x
  14  rsrch_dev       up     down    auto                network    10/100Base x
  15  rsrch_dev       up     down    auto                network    10/100Base x
  16  rsrch_dev       up     down    auto                network    10/100Base x
  17  rsrch_dev       up     down    auto                network    10/100Base x
  18  rsrch_dev       up     down    auto                network    10/100Base x
  19  mobility        up     up      auto      100/full  network    10/100Base x
  20  mobility        up     up      auto      100/full  network    10/100Base x
  21  backbone        up     down    auto                network
  22  backbone        up     down    auto                network
```

```
   6  conf_room1      up       MP    enabled    7.04
   7  conf_room2      up       MP    enabled    7.04
   8  manufacturing   up       MP    enabled    7.04
   9  manufacturing   up       MP    enabled    7.04
  10  manufacturing   up       MP    enabled    7.04
  11  manufacturing   up       MP    enabled    7.04
  12  manufacturing   up       MP    enabled    7.04
  13  manufacturing   up       MP    enabled    7.04
  14  rsrch_dev       up       MP    enabled    7.04
  15  rsrch_dev       up       MP    enabled    7.04
  16  rsrch_dev       up       MP    enabled    7.04
  17  rsrch_dev       down     -     disabled  off
  18  rsrch_dev       down     -     disabled  off
  19  mobility        down     -     disabled  off
  20  mobility        down     -     disabled  off
  21  backbone        down     -     -         invalid
  22  backbone        down     -     -         invalid
```

**4.** Configure ports 17 and 18 as wired authentication ports and verify the configuration change. Type the following commands:

```
MX# set port type wired-auth 17,18
success: change accepted
MX# show port status
Port  Name            Admin  Oper    Config    Actual     ype       Media
================================================================================
   1  mx_mgmt         up     up      auto      100/full  network    10/100Base x
   2  finance         up     up      auto      100/full  ap         10/100Base x
   3  accounting      up     up      auto      100/full  ap         10/100Base x
   4  shipping        up     up      auto      100/full  ap         10/100Base x
   5  lobby           up     up      auto      100/full  ap         10/100Base x
   6  conf_room1      up     up      auto      100/full  ap         10/100Base x
   7  conf_room2      up     up      auto      100/full  ap         10/100Base x
   8  manufacturing   up     up      auto      100/full  ap         10/100Base x
   9  manufacturing   up     up      auto      100/full  ap         10/100Base x
  10  manufacturing   up     up      auto      100/full  ap         10/100Base x
  11  manufacturing   up     up      auto      100/full  ap         10/100Base x
  12  manufacturing   up     up      auto      100/full  ap         10/100Base x
  13  manufacturing   up     up      auto      100/full  ap         10/100Base x
  14  rsrch_dev       up     up      auto      100/full  ap         10/100Base x
  15  rsrch_dev       up     up      auto      100/full  ap         10/100Base x
  16  rsrch_dev       up     up      auto      100/full  ap         10/100Base x
  17  rsrch_dev       up     up      auto      100/full  wired auth 10/100Base x
  18  rsrch_dev       up     up      auto      100/full  wired auth 10/100Base x
  19  mobility        up     up      auto      100/full  network    10/100Base x
  20  mobility        up     up      auto      100/full  network    10/100Base x
  21  backbone        up     down    auto                network
  22  backbone        up     down    auto                network
```

**5.** Configure ports 21 and 22 as a load-sharing port group to provide a redundant link to the backbone, and verify the configuration change. Type the following commands:

```
MX# set port-group name backbonelink port 21,22 mode on
success: change accepted.
MX# show port-group
Port group: backbonelink is up
        Ports:  22, 21
```

**6.** Add port 1 to the VLAN (VLAN 1), configure a VLAN named on ports 19 and 20, and verify the configuration changes. Type the following commands:

```
MX# set vlan default port 1
success: change accepted.
MX# set vlan 2 name roaming port 19-20
success: change accepted.
MX# show vlan config
                    Admin  VLAN   unl                          Port
VLAN Name           Status State Affin Port              ag    State
```

```
---- ---------------- ------ ----- ----- ---------------- ----- -----
   1 default          p      p        5
                                        1                none  p
   2 roaming          p      p        5
                                       19                none  p
                                       20                none  p
```

**7.** Save the configuration. Type the following command:

```
MX# save config
success: configuration saved.
```

The DHCP client is implemented according to “RFC 2131: Dynamic Host Configuration Protocol” and “RFC 2132: DHCP Options and BOOTP Vendor Extensions”. The client supports the following options:

- (12) Host Name (the MX system name)
- (55) Parameter request list, consisting of (1) Subnet Mask, (3) Router, (15) Domain Name, and (6) Domain Name Server
- (60) Vendor Class Identifier, set to TRPZ . . , where . . is the MSS version

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

```
clear interface vlan-id ip
```


The IP interface table flags the address assigned by a DHCP server with an asterisk ( * ). In the following example, VLAN received IP address 10.3.1.110 from a DHCP server.

```
MX# show interface
* = From DHCP
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- --------
   4 corpvlan        *10.3.1.110     255.255.255.0   YES      p    ipv4
Displaying DHCP Client Information
 o display DHCP client information, type the following command:
MX# show dhcp-client
 Interface:            corpvlan(4)
 Configuration Status: Enabled
 DHCP State:           IF_ P
 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
 DNS Servers:          10.3.1.29
 DNS Domain Name:      mycorp.com
```

### Disabling an IP Interface

IP interfaces are enabled by default. To administratively disable an IP interface, use the following command:

```
set interface vlan-id status {up | down}
```

### Removing an IP Interface

To remove an IP interface, use the following command:

```
clear interface vlan-id ip
```

### Displaying IP Interface Information

To display IP interface information, use the following command:

```
show interface [vlan-id]
```

## Configuring the System IP Address

You can designate one of the IP addresses configured on an MX to be the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:

- Mobility Domain operations
- Topology reporting for dual-homed MP access points

MSS can use a route only if the route is resolved by a direct route on one of the MX VLANs.

## Displaying IP Routes

To display IP routes, use the following command:

`show ip route [destination]`

The parameter specifies a destination IP address.

To display the IP route table, type the following command:

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

        0.0.0.0/ 0 Static       1 Router  10.0.1.17       vlan:1:ip
        0.0.0.0/ 0 Static       2 Router  10.0.2.17       vlan:2:ip
      10.0.1.1/24 IP            0 Direct                  vlan:1:ip
      10.0.1.1/32 IP            0 Local                   vlan:1:ip:10.0.1.1/24
    10.0.1.255/32 IP            0 Local                   vlan:1:ip:10.0.1.1/24
      10.0.2.1/24 IP            0 Direct                  vlan:2:ip
      10.0.2.1/32 IP            0 Local                   vlan:2:ip:10.0.2.1/24
    10.0.2.255/32 IP            0 Local                   vlan:2:ip:10.0.2.1/24
     224.0.0.0/ 4 IP            0 Local                   M L ICAS
```

```
     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                 M L ICAS
```

(For more information about the fields in the output, see the .)

## Adding a Static Route

SSH is enabled by default. Telnet and HTTPS are disabled by default.
An MX-20 or MX-400 can have up

## Adding an SSH User

To log in with SSH, a user must supply a valid username and password. To add a username and password to the local database, use the following command:

```
set user username password
```

Optionally, you also can configure MSS either to locally authenticate the user or to use a RADIUS server to authenticate the user. Use the following command:

```
set authentication admin {user-glob} method1 [method2] [method3] [method4]
```

To add administrative user with password , and use RADIUS server group to authenticate the user, type the following commands:

```
MX# set user mxadmin password letmein
success:  ser mxadmin created
MX# set authentication admin mxadmin sg1
success: change accepted
```

(For more information, see **"Adding and Clearing Local Users for Administrative Access" on page 6–8**.)

## Changing the SSH Service Port Number

To change the SSH port the MX switch listens on for SSH connections, use the following command:

```
set ip ssh port port-num
```


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 SSH port numbt to

## Managing SSH Server Sessions

Use the following commands to manage SSH server sessions:

```
show sessions admin
clear sessions admin ssh [session-id]
```

These commands display and clear SSH server sessions.

To display the SSH server sessions on an MX, type the following command:

```
MX# show sessions admin
 ty          sername                ime (s)     ype
-------     --------------------  --------     ----
tty0                              3644         Console
tty2        tech                  6             elnet
tty3        sshadmin              381          SSH

3 admin sessions
```

To clear all SSH server sessions, type the following command:

```
MX# clear sessions admin ssh
 his will terminate manager sessions, do you wish to continue? (y|n) [n]y
Cleared ssh session on tty3
```

(To manage Telnet client sessions, see **"Logging Into a Remote Device" on page 8–19**.)

These commands display and clear management sessions from a remote client to the MX Telnet server.


If you type the **clear sessions admin telnet** command from within a Telnet session, the session ends as soon as you press Enter.

To display the Telnet server sessions on an MX, type the following command:

```
MX# show sessions admin
 ty          sername               ime (s)     ype
-------     --------------------  --------    ----
tty0                              3644        Console
tty2        tech                  6            elnet
tty3        sshadmin              381         SSH

3 admin sessions
```

To clear all Telnet server sessions, type the following command:

```
MX# clear sessions telnet
 his will terminate manager sessions, do you wish to continue? (y|n) [n]y
Cleared telnet session on tty2
```

(To manage Telnet client sessions, see **"Logging Into a Remote Device" on page 8–19**.)

# Managing HTTPS

## Enabling HTTPS

HTTPS is disabled by default. To enable HTTPS, use the following command:

```
set ip https server {enable | disable}
```


If you disable the HTTPS server, Web View access to the MX is also disabled.

## Displaying HTTPS Information

To display HTTPS service information, use the following command:

```
show ip https
```

To display information for an MX HTTPS server, type the following command:

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

Last 5 Connections:
 IP Address     Last Connected          Last Activity (s)  ser       Secure
--------------- ---------------------- ----------------- ---------- ------
    172.16.7.84 2007/05/19 00:37:07 GM            5076789 session       YES
  172.21.36.250 2007/05/21 15:06:32 GM            4851824 session       YES
   172.21.26.91 2007/05/23 22:44:10 GM            4651566 session       YES
   172.21.26.65 2007/07/11 13:45:38 GM             450278 session       YES
   172.21.26.96 2007/07/16 18:48:11 GM                125 session       YES
```

The command lists the TCP port number that the MX listens for HTTPS connections. The command also lists the last 5 devices to establish HTTPS connections with the MX, when the connections were established, last activity, user accessing through HTTPS, and if the connection is secure.

If a browser connects to an MX from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output.

## Changing the Idle Timeout for CLI Management Sessions

By default, MSS automatically terminates an console or Telnet session that is idle for more than one hour. To change the idle timeout for CLI management sessions, use the following command:

```
set system idle-timeout seconds
```

You can specify from 0 to 86400 seconds (one day). The default is 3600 (one hour). If you specify 0, the idle timeout is disabled. The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval

The is displayed at the end of the MOTD, and can be up to 32 characters in length. In response, the user has the option of entering **y** to proceed or any other key to terminate the connection.

The following command enables the prompt for the MOTD banner:

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

The following command sets as the text to be displayed following the MOTD banner:

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

After these commands are entered, and a 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.
```

# Configuring and Managing DNS

You can configure an MX to use a Domain Name Service (DNS) server to resolve hostnames into IP addresses. This capability is useful in cases when you specify a hostname instead of an IP address in a command.

For example, as an alternative to the command **ping 192.168.9.1**, you can enter the command **ping chris.example.com**. When you enter **ping chris.example.com**, the MX DNS client queries a DNS server for the IP address corresponding to the hostname , then sends the ping request to that IP address.

The DNS client on the MX is disabled by default. To configure DNS:

- Enable the DNS client.
- Specify the IP addresses of the DNS servers.
- Configure a default domain name for DNS queries.

## Enabling or Disabling the DNS Client

The DNS client is disabled by default. To enable or disable the DNS client, use the following command:

```
set ip dns {enable | disable}
```

## Configuring DNS Servers

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

The MX always sends a request to the primary DNS server first. The MX sends a request to a secondary DNS server only if the primary DNS server does not respond.

### Adding a DNS Server

To add a DNS server, use the following command:

```
set ip dns server ip-addr {primary | secondary}
```

### Removing a DNS Server

To remove a DNS server, use the following command:

```
clear ip dns server ip-addr
```

## Configuring a Default Domain Name

You can configure a single default domain name for DNS queries. The MX appends the default domain name to hostnames entered in commands. For example, you can configure the MX to automatically append the domain name to any hostname without a domain name. In this case, you can enter **ping chris** instead of **ping chris.example.com**, and the MX automatically requests the DNS server to send the IP address for .

To override the default domain name when entering a hostname

. mrexoamp the efault domain name, ent er chrt.m his

```
success: change accepted.
```

After configuring the alias, you can use in commands in place of the IP address. For example, to ping 192.168.1.2, you can type the command **ping HR1**.

### Removing an Alias

To remove an alias, use the following command:

```
clear ip alias name
```

### Displaying Aliases

To display aliases, use the following command:

```
show ip alias [name]
```

Here is an example:

```
MX# show ip alias
Name                    IP Address
--------------------    --------------------
HR1                     192.168.1.2
payroll                 192.168.1.3
radius1                 192.168.7.2
```

## Configuring and Managing Time Parameters

You can configure the system time and date statically or by using Network Time Protocol (NTP) servers. In each case, you can specify the offset from Coordinated Universal Time (UTC) by setting the time zone. You also can configure MSS to offset the time by an additional hour for daylight savings time or similar summertime period.


Trapeze Networks recommends that you set the time and date parameters before you install certificates on the MX. If the MX time and date are incorrect, the certificate may not be valid.

Generally, CA-generated certificates are valid for one year beginning with the system time and date that are in effect when you generate the certificate request. Self-signed certificates generated by MSS Version 4.2.3 or later are valid for three years, beginning one week before the time and date on the MX when the certificate is generated.

If you do not install certificates, the MX automatically generates them the first time you boot the MX with MSS Version 4.2 or later. The automatically generated certificates are dated based on the time and date information present on the MX when it is first booted with MSS Version 4.2 or later.

To statically set the time and date:

- Set the time zone (**set timezone**)
- Set the summertime period (**set summertime**)
- Set the time and date (**set timedate**)

To use NTP servers to set the time and date:

- Set the time zone (**set timezone**)
- Set the summertime period (**set summertime**)
- Configure NTP server information (**set ntp** commands)

### Setting the Time Zone

The time zone parameter adjusts the system date, and optionally the time, by applying an offset to UTC.

For example, to display the summertime period, type the following command:

```
MX# show summertime
Summertime is enabled, and set to 'PD '.
  Start  : Sun Apr 04 2004, 02:00:00
  End    : Sun Oct 31 2004, 02:00:00
  Offset : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
              and ending at 2:00 am on last Sunday of October.
```

(For information about the fields in the output, see the
)

### Clearing the Summertime Period

To clear the summertime period, use the following command:

```
clear summertime
```

## Statically Configuring the System Time and Date

The NTP client is disabled by default.

## Adding an NTP Server

To add an NTP server to the list of NTP servers, use the following command:

```
set ntp server ip-addr
```

To configure an MX to use NTP server 192.168.1.5, type the following command:

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

## Removing an NTP Server

To remove an NTP server, use the following command:

```
clear ntp server {ip-addr | all}
```

If you use the **all** option, MSS clears all NTP servers configured on the MX.

## Changing the NTP Update Interval

The default update interval is 64 seconds. To change the update interval, use the following command:

```
set ntp update-interval seconds
```

You can specify an interval from 16 through 1024 seconds.

For example, to change the NTP update interval to 128 seconds, type the following command:

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

## Resetting the Update Interval to the Default

To reset the update interval to the default value, use the following command:

```
clear ntp update-interval
```

## Enabling the NTP Client

The NTP client is disabled by default. To enable the NTP client, use the following command:

```
set ntp {enable | disable}
```

## Displaying NTP Information

To display NTP information, use the following command:

```
show ntp
```

Here is an example:

```
MX> show ntp
N P client: enabled
Current update-interval: 20(secs)
Current time: Sun Feb 29 2004, 23:58:12
 imezone is set to 'PS ', offset from   C is -8:0 hours.
Summertime is enabled.
Last N P update: Sun Feb 29 2004, 23:58:00
N P Server          Peer state          Local State
-------------------------------------------------
192.168.1.5         SYSPEER             SYNCED
```

The Timezone and Summertime fields are displayed only if you change the timezone or enable summertime.

(For more information about the fields in the output, see the
)

# Managing the ARP Table

The Address Resolution Protocol (ARP) table maps IP addresses to MAC addresses. An ARP entry enters the table in one of the following ways:

- Added automatically by the MX. The MX adds an entry for the MAC address and adds entries for addresses learned from received network traffic. When the MX receives an IP packet, the MX adds the packet source MAC address and source IP address to the ARP table.
- Added by the system administrator. You can add dynamic, static, and permanent entries to the ARP table.

ARP is enabled by default on an MX and cannot be disabled.

## Displaying ARP Table Entries

To display ARP table entries, use the following command:

```
show arp [ip-addr]
```

Here is an example:

```
MX# show arp
ARP aging time: 1200 seconds

Host                          HW Address        VLAN   ype    State
----------------------------- ----------------- ----- ------- --------
10.5.4.51                     00:0b:0e:02:76:f5     1 DYNAMIC RESOLVED
10.5.4.53                     00:0b:0e:02:76:f7     1 LOCAL   RESOLVED
```

This example shows two entries. The local entry (with LOCAL in the Type field) is for the MX. The MAC address of the local entry is the MX MAC address. The ARP table contains one local entry for each VLAN configured on the switch. The dynamic entry is obtained from traffic received by the MX. The ARP table can also contain static and permanent entries, added by an administrator. The State field indicates whether an entry is resolved (RESOLVED) or whether MSS has sent an ARP request for the entry and is waiting for the reply (RESOLVING).

## Adding an ARP Entry

MSS automatically adds a local entry for an MX and dynamic entries for addresses obtained from traffic received by the MX. You can add the following types of entries:

- Dynamic—Expires based on the aging timeout.
- Static—Does not expire but is removed by a software reboot.
- Permanent—Does not expire and remains in the ARP table following a software reboot.

To add an ARP entry, use the following command:

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

To add a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff, type the following command:

```
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
```

## Changing the Aging Timeout

The aging timeout specifies how long a dynamic entry can remain unused before the software removes the entry from the ARP table. The default aging timeout is 1200 seconds (20 minutes). The aging timeout does not affect the local entry, static entries, or permanent entries.

To change the aging timeout, use the following command:

```
set arp agingtime seconds
```

You can specify from 0 to 1,000,000 seconds. To disable aging, specify 0.

For example, to disable aging of dynamic ARP entries, type the following command:

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


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

## Pinging Another Device

To verify that another device in the network can receive IP packets sent by the MX, use the following command:

```
ping host [count num-packets] [dnf] [flood] [interval time] [tos tos] [user user]
```

To ping a device that has IP address 10.1.1.1, type the following command:

```
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
```

In this example, the ping is successful, indicating IP connectivity with the other device.

(For information about the command options, see the
)

## Logging Into a Remote Device

From within an MSS console session or Telnet session, you can use the Telnet client to establish a Telnet client session from an MX to another device. To establish a Telnet client session with another device, use the following command:

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

To establish a Telnet session from MX switch to 10.10.10.90, type the following command:

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

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

 sername:
```

When you press Ctrl+t or type **exit** to end the client session, the management session returns to the local MX prompt:.

```
MX-remote> Session 0 pty tty2.d terminated tt name tty2.d
MX#
```

Use the following commands to manage Telnet client sessions:

```
show sessions telnet client
clear sessions telnet client [session-id]
```

These commands display and clear Telnet sessions from an MX Telnet client to another device.

To display the Telnet client sessions on an MX, type the following command:

```
MX# show sessions telnet client
Session   Server Address    Server Port    Client Port
-------   --------------    ------------   -----------
0          192.168.1.81     23             48000
1           10.10.1.22      23             48001
```

To clear Telnet client session 0, type the following command:

```
MX# clear sessions telnet client 0
```

You also can clear a Telnet client session by typing **exit** from within the client session.

# IP Interfaces and Services Configuration Scenario

This scenario configures IP interfaces, assigns the system IP address to an interface, and configures a default route, DNS parameters, and time and date parameters.

1. Configure IP interfaces on the and VLANs, and verify the configuration changes. Type the following commands:

```
MX# set interface mx_mgmt ip 10.10.10.10/24
success: change accepted.
MX# set interface roaming ip 10.20.10.10/24
success: change accepted.
MX# show interface
* = From DHCP
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- --------
   1 default         10.10.10.10     255.255.255.0   YES       p    ipv4
   2 roaming         10.20.10.10     255.255.255.0   YES       p    ipv4
```

2. Configure the IP interface on the VLAN to be the system IP address and verify the configuration change. Type the following commands:

```
MX# set system ip-address 10.20.10.10
success: change accepted.
MX# show system
================================================================================
 Product Name:       MX
 System Name:        MX
 System Countrycode:  S
 System Location:
 System Contact:
 System IP:          10.02.10.10
 System idle timeout:3600
 System MAC:         00:0B:0E:00:04:0C
================================================================================
 Boot  ime:          2000-03-18 22:59:19
```

```
    10.10.10.10/32 IP          0 Local                  vlan:1:ip:10.10.10.10/24
    10.20.10.10/24 IP          0 Direct                 vlan:1:ip
    10.20.10.10/32 IP          0 Local                  vlan:1:ip:10.20.10.10/24
      224.0.0.0/ 4 IP          0 Local                  M L ICAS
Configure the DNS domain name and DNS server entries,and enable the DNS service. And
        verify the configuration changes.  ype the following commands:
MX# set ip dns domain example.com
success: change accepted.
MX# set ip dns server 10.10.10.69 PRIMARY
success: change accepted.
MX# set ip dns server 10.20.10.69 SECONDARY
success: change accepted.
MX# set ip dns enable
success: change accepted.
MX# show ip dns
Domain Name: example.com
DNS Status: enabled
IP Address                ype
---------------------------------
10.10.10.69              PRIMARY
10.20.10.69              SECONDARY
```

**4.** Configure time zone, summertime, and NTP parameters and verify the configuration changes. Type the following commands:

```
MX# set timezone PS  -8
success: change accepted.
MX# show timezone
 imezone is set to 'PS ', offset from   C is -8:0 hours.
MX# set summertime PD
success: change accepted.
MX# show summertime
Summertime is enabled, and set to 'PD '.
  Start  : Sun Apr 04 2004, 02:00:00
  End    : Sun Oct 31 2004, 02:00:00
  Offset : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
              and ending at 2:00 am on last Sunday of October.
MX# set ntp server 192.168.1.5
MX# set ntp enable
success: N P Client enabled
MX# show ntp
N P client: enabled
Current update-interval: 20(secs)
Current time: Sun Feb 29 2004, 23:58:12
 imezone is set to 'PS ', offset from   C is -8:0 hours.
Summertime is enabled.
Last N P update: Sun Feb 29 2004, 23:58:00
N P Server          Peer state          Local State
-----------------------------------------------------
192.168.1.5         SYSPEER             SYNCED
MX# show timedate
Sun Feb 29 2004, 23:59:02 PS
```

**5.** Save the configuration. Type the following command:

```
MX# save config
success: configuration saved.
```

# DHCP Server

The MX has a DHCP server that is used to allocate IP addresses to the following items and is enabled by default:

- Directly connected MPs
- Host connected to a new (unconfigured) MXR-2, MX-8, MX-200, or MX-216, to configure the MX using the Web Quick Start.

Optionally, you can configure the DHCP server to also provide IP addresses to Distributed MPs and to clients.

Configuration is supported on an individual VLAN basis. When you configure the DHCP server on a VLAN, the server can distributes addresses only from the subnet with the host address assigned to the VLAN. By default, the VLAN can serve any unused address in the subnet except the VLAN host address and the network and broadcast addresses. You can specify the address range.

You can configure the DHCP server for more than one VLAN. 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.

The MSS DHCP server is implemented according to “RFC 2131: Dynamic Host Configuration Protocol” and “RFC 2132: DHCP Options and BOOTP Vendor Extensions”, with the following exceptions:

- If the MX is powered down or restarted, MSS does not retain address allocations or lease times.
- The MSS DHCP server does not operate properly when another DHCP server is present on the same subnet.
- The MSS DHCP server is configurable on an individual VLAN basis only, and operates only on the subnets that you configure it.

## How the MSS DHCP Server Works

When MSS receives a DHCP Discover packet, the DHCP server allocates an address from the configured range according to RFC 2131 and sends an ARP message to the address to be sure that it is available on the network. If the address is in use, the server allocates the next address in the range, and resends ARP message again. The process continues until MSS finds an unused address. MSS then offers the address to the Distributed MP or client that sent the DHCP Discover. If there are no unused addresses left in the range, MSS ignores the DHCP Discover and generates a log message.

If the client does not respond to the DHCP Offer from the MSS DHCP server within 2 minutes, the offer becomes invalid and MSS returns the address to the pool.

The value in the DHCP exchanges is the IP address of the VLAN. The value is an unused address within the range the server is allowed to use.

In addition to an IP address, the Offer message from the MSS DHCP server also contains the following options:

- Option 54—Server Identifier, that has the same value as siaddr.
- Option 51—Address Lease, which is 12 hours and cannot be configured.
- Option 1—Subnet Mask of the IP interface of the VLAN.
- Option 15—Domain Name. If this option is not set with the **set interface dhcp-server** command **dns-domain** option, the MSS DHCP server uses the value set by the **set ip dns domain** command.
- Option 3—Default Router. If this option is not set with the **set interface dhcp-server** command **default-router** option, the MSS DHCP server can use the value set by the **set ip route** command. A default route configured by **set ip route** can be used if the route is in the DHCP client subnet. Otherwise, the MSS DHCP server does not specify a router address.
- Option 6—Domain Name Servers. If these options are not set with the **set interface dhcp-server** command **primary-dns** and **secondary-dns** options, the MSS DHCP server uses the values set by the **set ip dns server** command.

# Configuring the DHCP Server

You can configure the DHCP server on an individual VLAN basis. To configure the server, use the following command:

```
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]
```

The can be the VLAN name or number.

The **start** and **stop** options specify the beginning and ending IP addresses of the IP address range (also called the address ). 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.

(For information about the other options, see the )

The following command enables the DHCP server on VLAN to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
MX# set interface red-vlan ip dhcp-server enable start 192.168.1.5 stop 192.168.1.25
success: change accepted.
```

To remove all IP information from a VLAN, including the DHCP client and user-configured DHCP server, use the following command:

```
clear interface vlan-id ip
```


This command clears all IP configuration information from the interface.

# Displaying DHCP Server Information

To display information about the MSS DHCP server, use the following command:

```
show dhcp-server [interface vlan-id] [verbose]
```

If you enter the command without the interface or verbose option, the command displays a table of all the IP addresses leased by the server. You can use the **interface** option to display addresses leased by a specific VLAN.

If you use the **verbose** option, configuration and status information is displayed instead.

The following command displays the addresses leased by the 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
 he following command displays configuration and status information for each VLAN on
         which the DHCP server is configured:
MX# show dhcp-server verbose
Interface:        0 (Direct AP)
 Status:           P
 Address Range:    10.0.0.1-10.0.0.253

 Interface:           default(1)
 Status:               P
 Address Range:       10.10.20.2-10.10.20.254

Hardware Address:     00:01:02:03:04:05
   State:               BO ND
   Lease Allocation:    43200 seconds
   Lease Remaining:     12345 seconds
   IP Address:          10.10.20.2
   Subnet Mask:         255.255.255.0
   Default Router:      10.10.20.1
   DNS Servers:         10.10.20.4 10.10.20.5
   DNS Domain Name:     mycorp.com
```

In addition to information for addresses leased from the VLANs where the server is configured, information for the Direct AP interface is also displayed. The Direct AP interface is an internal VLAN interface for directly connected MPs.

# Configuring SNMP

MSS supports Simple Network Management Protocol (SNMP) versions 1, 2c, and 3.

## Overview

The MSS SNMP engine (also called the SNMP or ) can run any combination of the following SNMP versions:

- SNMPv1—SNMPv1 is the simplest and least secure SNMP version. Community strings are used for authentication. Communications are in the clear (not encrypted). Notifications are traps, which are not acknowledged by the notification target (also called a ).
- SNMPv2c—SNMPv2 is similar to SNMPv1, but supports informs. An inform is a notification that is acknowledged by the notification target.
- SNMPv3—SNMPv3 adds authentication and encryption options. Instead of community strings, SNMPv3 supports user security model (USM) users, with individually configurable access levels, authentication options, and encryption options.

All SNMP versions are disabled by default.

## Configuring SNMP

To configure SNMP, perform the following tasks:

- Set the MX IP address, if it is not already set. SNMP does not work without the system IP address.
- Set the system location and contact strings.(Optional)
- Enable the SNMP version(s) to use on the network. MSS can run one or more versions, in any combination.
- Configure community strings (for SNMPv1 or SNMPv2c) or USM users (for SNMPv3).
- Set the minimum level of security allowed for SNMP message exchanges.
- Configure a notification profile or modify the default one, to enable sending of notifications to notification targets. By default, notifications of all types are not sent.
- Configure notification targets.
- Enable the MSS SNMP engine.
- If you require compliance with the US Army TIC, configure monitor and admin as roles.

### Setting the System Location and Contact Strings

To set the location and contact strings for an MX, use the following commands:

```
set system location string
set system contact string
```

Each string can be up to 256 characters long, with no blank spaces.

The following commands set an MX location to and set the contact to :

```
MX# set system location 3rd_floor_closet
success: change accepted.
MX# set system contact sysadmin1
success: change accepted.
```

Configuring SNMP

- **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 MX system IP address.

The **access** option specifies the access level of the user. The options are identical to the access options for community strings. (See **"Configuring Community Strings (SNMPv1 and SNMPv2c Only)" on page 9–2**.) The default is **read-only**.

The **auth-type** option specifies the authentication type used to authenticate communications with the remote SNMP engine. You ca

To assign a role to the SNMP group, use the following command:

```
MX# set snmp community name comm-string group [monitor | admin]
```

## Defining SNMP Views

You can configure SNMP views and apply them to users and communities. To create a view, use the following command:

```
MX# set snmp view view-name description view-description
```

The description option allows you to add security view information that allows you to identify individual views. For instance, you may want to create two views for SNMP, such as security level 1 and security level 2.

```
MX# set snmp view securitylevel1 description limitedviews
success: change accepted.

MX# set snmp view securitylevel2 description view-all
```

There are three predefined views: **all**, **hideSec**, and **setSys**. The view, **all**, contains all objects that are readable or writeable in the SNMP agent. The view, **hideSec**, does not display the SNMP security configuration information. All other objects are allowed. The view, **setSys**, restricts the set command to required instrumentation code such as sysName, sysLocation, and sysContact.

An OID is an object identifier for an object in a Management Information Base (MIB). A newly created view does not contain any tree families so you must add tree families to the view. Use the following command:

```
MX# set snmp view view-name treefamily oid-subtree
```

To match all OIDs, use the additional root option as follows:

```
MX# set snmp view view-name root {included | excluded}
```

## Displaying SNMP Group Information

Use the following command to display all configured SNMP groups on the MX:

```
MX# show snmp group all

                 Sec.  Sec.
Group name       model level    Read view       Write view      Notify view
---------------- ----- -------- --------------- --------------- --------------
*monitor         V1    -        hideSec         -               all
*monitor         V2C   -        hideSec         -               all
*monitor          SM   -        hideSec         -               all
*monitor          SM   Auth     hideSec         -               all
*monitor          SM   AuthPriv hideSec         -               all
*admin           V1    -        all             setSys          all
*admin           V2C   -        all             setSys          all
*admin            SM   -        all             setSys          all
*admin            SM   Auth     6.7(    all)] J *[(*ad)6.7(min     )6.7(      V1)6.7(    -    )6.
```

## Configuring a Notification Profile

A is a named list of all the notification types that can be generated by an MX, and for each notification type, the action, drop or send, to perform when an event occurs.

A default notification profile (named ) is already configured in MSS. All notifications in the default profile are dropped by default. You can configure up to 10 notification profiles.

To modify the default notification profile or create a new one, use the following command:

```
set snmp notify profile {default | notify-profile-name} {drop | send} {notifica-
        tion-type | all}
```

To clear a notification profile, use the following command:

```
clear snmp notify profile profile-name
```

The can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify **default**.

The can be one of the following:

- **ApNonOperStatusTraps**—Generated to indicate an MP radio is nonoperational.
- **ApOperRadioStatusTrap2**—Generated when the status of an MP radio changes.
- **ApRejectLicenseExceededTraps**—Generated when the number of MPs exceed the licensed number.
- **AuthenTraps—**Generated when the MX 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 attempts to associate with a radio and fails.
- **ClientAssociationSuccessTraps**—Generated when a client association is successful.
- **ClientAuthenticationSuccessTraps—**Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps—**Generated when authentication fails for a client.
- **ClientAuthorizationFailureTraps—**Generated when authorization fails for a client.
- **ClientAuthorizationSuccessTraps—**Generated when authorization is successful for a client.
- **ClientClearedTraps—**Generated when a client 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 network.
- **ClientDot1xFailureTraps—**Generated when a client experiences an 802.1X failure.
- **ClientDynAuthorChangeFailureTrap**s—Generated when a dynamic RADIUS client fails to authenticate.
- **ClientDynAuthorChangeSuccessTraps**—Generated when a dynamic RADIUS client has a successful authentication.
- **ClientIPAddrChangeTraps**—Generated when the IP address for a client changes on the network.
- **ClientRoamingTraps—**Generated when a client roams.
- ConfigurationsSavedTraps**—Generated when a configuration is saved on the MX.**
- **CounterMeasureStartTraps—**Generated when MSS begins countermeasures against a rogue access point.
- **CounterMeasureStopTraps—**Generated when MSS stops countermeasures against a rogue access point.
- **DeviceFailTraps—**Generated when an event with an Alert severity occurs.

Configuring SNMP

- **DeviceOkayTraps—**Generated when a device re

The **drop** or **send** option specifies the action that the SNMP engine takes with regard to notifications.

### Command 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 RFDetectAdhoc ser raps
success: change accepted.

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

MX# set snmp notify profile snmpprof_rfdetect send RFDetectClientViaRogueWiredAP-
          raps
success: change accepted.

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

MX# set snmp notify profile snmpprof_rfdetect send RFDetectAdhoc serDisappear raps
success: change accepted.

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

MX# set snmp notify profile snmpprof_rfdetect send RFDetectInterferingRogueDisap-
         pear raps
success: change accepted.

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

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

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

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

MX# set snmp notify profile snmpprof_rfdetect send RFDetect nAuthorizedAP raps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetect nAuthorizedOui raps
success: change accepted.

MX# set snmp notify profile snmpprof_rfdetect send RFDetect nAuthorizedSsid raps
success: change accepted.
```

## Configuring a Notification Target

A notification target is a remote device to which MSS 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.

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

Configuring SNMP

retries. The default is 0. The **timeout** option specifies the number of seconds MSS waits for

# Configuring Communication with RADIUS

For a list of the standard and extended RADIUS attributes and Trapeze vendor-specific attributes (VSAs) supported by MSS, see Appendix , “,” on page C-1.

## RADIUS Overview

Remote Authentication Dial-In User Service (RADIUS) is a distributed client-server system. RADIUS servers provide a repository for all usernames and passwords, and can manage and store large groups of users.

RADIUS servers store user profiles that include usernames, passwords, and other AAA attributes. You can use authorization attributes to authorize users for a type of service, for appropriate servers and network segments through VLAN assignments, for packet filtering by access control lists (ACLs), and for other services during a session.

You must include RADIUS servers in a server group before you can access the servers.

5. If the client does not support 802.1X, MSS attempts to perform MAC authentication for the client instead. In this case, if the MX configuration contains a **set authentication mac** command that matches the client MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

## Before You Begin

To ensure that you can contact the RADIUS servers you plan to use for authentication, send the **ping** command to each one to verify connectivity.

```
ping ip-address
```

You can then set up communication between the MX and each RADIUS server group.

## Configuring RADIUS Servers

An authentication server validates each client with access to an MX port before any services are available on the MX or the wireless network. The

For failover authentication or authorization to work promptly, Trapeze Networks recommends that you change the dead time to a value other than 0. With the default setting, the dead time is never invoked and MSS does not hold down requests to unresponsive RADIUS servers. Instead, MSS attempts to send each new authentication or authorization request to a server even if the server appears unresponsive. This behavior can cause authentication or authorization failures on clients because MSS does not fail over to the local method quickly and the clients eventually time out.

## Configuring Global RADIUS Defaults

You can change RADIUS values globally and set a global password (key) with the following command. The key is the shared secret that the MX uses to authenticate to the RADIUS server.

```
set radius {deadtime minutes | encrypted-key string | key string | retransmit number
        | timeout seconds}
```

(To override global settings for individual RADIUS servers, use the **set radius server** command. See **"Configuring Individual RADIUS Servers" on page 10–3**.)

For example, the following commands set the dead-time timer to 10 minutes and set the password to for all RADIUS servers in the MX configuration:

```
MX# set radius deadtime 10
success: change accepted.
MX# set radius key r8gney
success: change accepted.
```

To reset global RADIUS server settings to their factory defaults, use the following command:

```
clear radius {deadtime | key | retransmit | timeout}
```

For example, the following command resets the dead-time timer to 0 minutes on all RADIUS servers in the MX configuration:

```
MX# clear radius deadtime
success: change accepted.
```

## Setting the System IP Address as the Source Address

By default, RADIUS packets leaving the MX have the source IP address of the outbound interface on the MX. The source address can change when routing conditions change. If you set a system IP address for the MX, you can use it as a permanent source address for the RADIUS packets sent by the MX.

To set the MX system IP address as the address of the RADIUS client, type the following command:

```
MX# set radius client system-ip
success: change accepted.
```

To remove the MX system IP address as the source address in RADIUS client requests from the MX to the RADIUS server(s), type the following command:

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

The command causes the MX to select a source interface address based on routing table information as the RADIUS client address.

## Configuring Individual RADIUS Servers

You must set up a name and IP address for each RADIUS server. To configure a RADIUS server, use the following command:

```
set radius server server-name [address ip-address] [key string]
```

The server name must be unique for this RADIUS server on the MX. Do not use the same name for a RADIUS server and a RADIUS server group. The key (password) is the shared secret that the MX uses to authenticate to the RADIUS server. (For additional options, see the .)

For MSS Version 6.2, additional attributes must be configured on the RADIUS server. For the user-group name, specify a value consisting of a string 1-32 characters long. Additional values consist of Type - 26, Vendor ID- 14525, Vendor Type - 9 (Trapeze VSA).

Attributes that appear in the RADIUS Access Accept response are added to the session attributes. If the Access Accept has a Trapeze group-name VSA, the attributes from the corresponding user group in the local database are applied.

## Configuring RADIUS Server Groups

A server group is a group of up to four RADIUS servers. Before you can use a RADIUS server for

## Configuring Load Balancing

You can configure the MX to distribute authentication requests across RADIUS servers in a server group. Distributing the authentication process across multiple RADIUS servers significantly reduces the load on individual servers while increasing resiliency on a system-wide basis.

When you configure load balancing, the first client RADIUS requests are directed to the first server in the group, the second client RADIUS requests are directed to the second server in the group, and so on. When the last server in the group is reached, the cycle is repeated.

To configure load balancing, use the following command:

```
set server group group-name load-balance enable
```

For example, to configure RADIUS servers and as the server group with load balancing:

1. Configure the members of a server group by typing the following command:

```
MX# set server group swampbirds members pelican seagull
success: change accepted.
```

2. Enable load balancing by typing the following command:

```
MX# set server group swampbirds load-balance enable
success: change accepted.
```

The following command disables load balancing for a server group:

```
clear server group group-name load-balance
```

## Adding Members to a Server Group

To add RADIUS servers to a server group, type the following command:

```
set server group group-name members server-name1 [server-name2] [server-name3]
        [server-name4]]
```

The keyword **members** lists the RADIUS servers contained in the named server group. A server group can contain between one and four RADIU

**6.** Display the configuration. Type the following command:

```
MX# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)
Radius Servers
Server                  Addr           Ports    /o  ries Dead State
-------------------------------------------------------------------
sandpiper            192.168.253.17  1812 1813  5    3    0     P
seagull              192.168.243.12  1812 1813  5    3    0     P
egret                192.168.243.15  1812 1813  5    3    0     P
pelican              192.168.253.11  1812 1813  5    3    0     P
Server groups
    swampbirds (load-balanced): pelican seagull
    shorebirds (load-balanced): egret pelican sandpiper
```

## Dynamic RADIUS Extensions

This feature allows administrators supporting a RADIUS server to disconnect a user and change the authorization attributes of an existing user session. New terminology is introduced in support of RFC 4673 (Dynamic Authorization Server MIB):

- **Dynamic Authorization Server (DAS)** — The component residing on the NAS and processes the Disconnect and Change-of-Authorization (CoA) requests sent by the Dynamic Authorization Client (DAC).
- **Dynamic Authorization Client (DAC)** — The component residing sending the Disconnect and CoA requests to the DAS. Though the DAC often resides on the RADIUS server, it can be located on a separated host, such as a rating engine.
- **Dynamic Authorization Server Port** — The UDP that the DAS listens for Disconnect and CoA requests sent by the DAC.

### Configuration

To configure a RADIUS DAC server on an MX, use the following commands:

```
MX# set radius dac dac-name ip-address key <string>
```

Additional attributes include the following:

```
[disconnect [enable | disable] | [change-of-author [enable | disable] | replay-pro-
        tection [enable | disable] | replay-window seconds ]
```

To configure the dynamic authorization server port, use the following command:

```
MX# set radius das-port portnum
```

To clear the das-port, use the following command:

```
MX# clear radius das-port
```

To configure SSIDs for RADIUS DAC, use the following commands:

```
MX# set authorization dynamic {ssid [wireless_8021X | 8021x | any |<name>]| wired
        <name>}
```

You can configure up to four SSIDs and four wired rule names for RADIUS DAC.

### `termination-action` Attribute for RADIUS

The termination-action RADIUS attribute is now supported in MSS 7.0. This attribute support reauthentication of all access types: dot1x, web-portal, MAC, and last-resort. When the value is

## MAC Authentication Request Format

### Description

MAC Authentication Request is an enhancement to the current username and password format available in MSS for authentication through a RADIUS server. Changes to this feature allow for

11

# Configuring AAA for Network Users

## About AAA for Network Users

Network users include the following types of users:

- Wireless users—Users who access the network by associating with an SSID on a Trapeze radio.
- Wired authentication users—Users who access the network over an Ethernet connection to an MX switch port that is configured as a wired authentication ( ) port.
- Local users that log into the MX for administrative access.

You can configure authentication rules for each type of user, on an individual SSID or wired authentication port basis. MSS authenticates users based on user information on RADIUS servers or on the local database of the MX. The RADIUS servers or local database authorizes successfully authenticated users for specific network access, including VLAN membership. Optionally, you also can configure accounting rules to track network access information.

The following sections describe the MSS authentication, authorization, and accounting (AAA) features in more detail.

### Authentication

When a user attempts to access the network, MSS checks for an authentication rule that matches the following parameters:

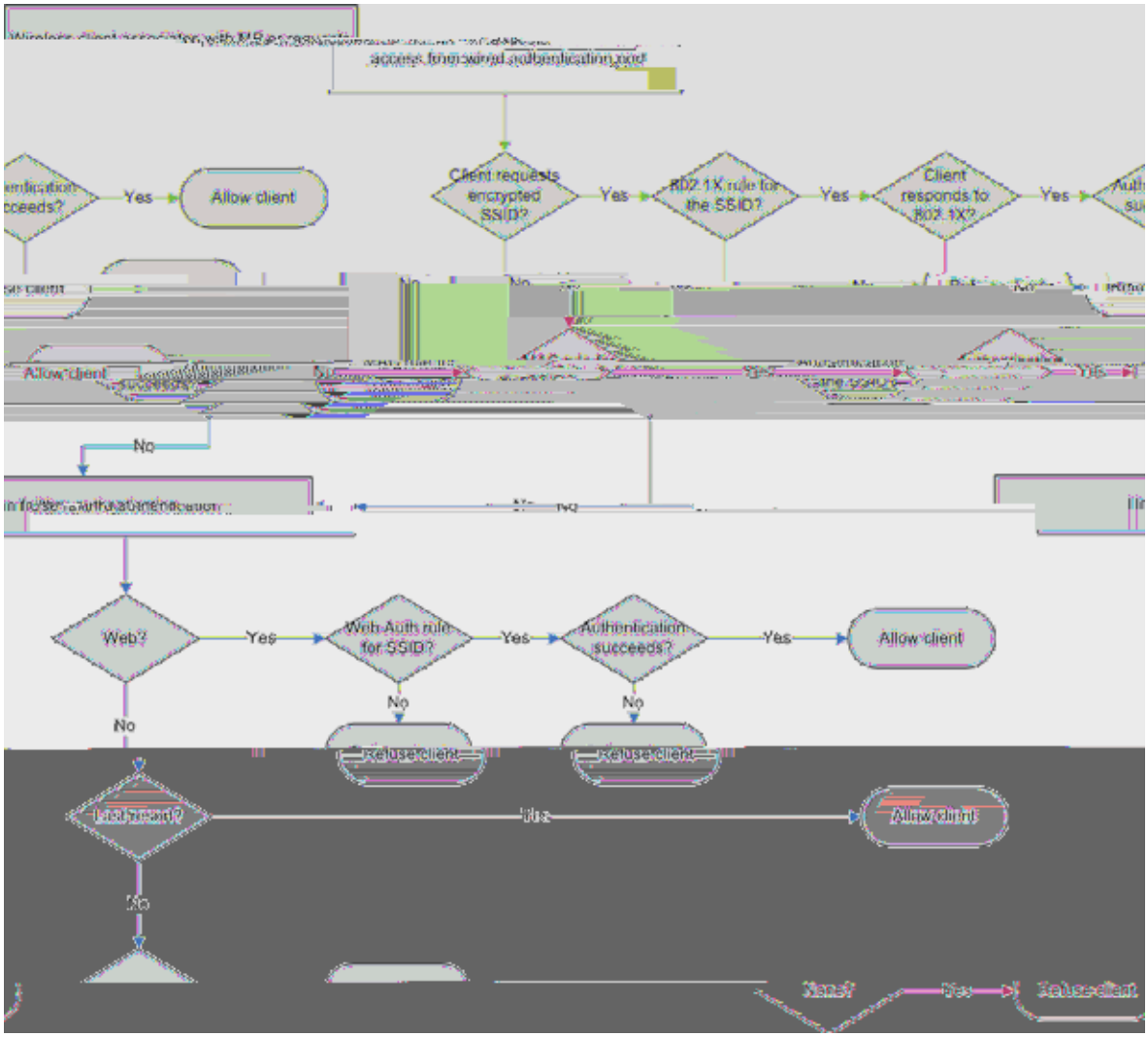
- For wireless access, the authentication rule must match the user-requested SSID, and the username or MAC address.
- For access on a wired authentication port, the authentication rule must match the username or MAC address.

If a matching rule is found, MSS then checks the RADIUS servers or the local database on the MX for credentials matching those presented by the user. Depending on the type of authentication

- MAC—If the username does not match an 802.1X authentication rule, but the MAC address of the NIC or Voice-over-IP (VoIP) phone and the SSID (if wireless) do match a MAC authentication rule, MSS checks the RADIUS server group or local database for matching user information. If the MAC address (and password, if on a RADIUS server) matches, MSS grants access. Otherwise, MSS attempts the fallthru authentication type, which can be Web, last-resort, or none. (Fallthru authentication is described in more detail in **"Authentication Algorithm" on page 11–2**.)
- Web—A network user attempts to access a Web page over the network. The MX intercepts the HTTP or HTTPS request and displays a login Web page to the user. The user enters the username and password, and MSS checks the RADIUS server group or local database for matching user information. If the username and password match, MSS redirects the user to the requested Web page. Otherwise, MSS denies access to the user.
- Last-resort—A network user associates with an SSID or connects to a wired authentication port, and does not enter a username or password.
  - SSID—If no 802.1X or MAC access rules are configured for the SSID, the default authorization attributes set on the SSID are applied to the user and the user is allowed onto the network.
  - Wired authentication port—If 802.1X or MAC authentication does not apply to the port (no 802.1X or MAC access rules have the **wired** option set), MSS checks for user

. 1ccese user ic6(o)-5.1f1(ig)-2.9(ud,on)-4.4cces(au5(oi)]TJ1945578 0 TD.0516 Tc-.0003 Twi
TD.0021 Tc.0286 TwOo thlie-4.8( )6(M7-9.S(.)-2.MSattute( the)-9(er )]TJ/TT16 1 T12-..241 0 Tc0 Tw2(fa4.6(l)-4.2(l)8.1(t3)4.3()-2.ru–2)

**Figure 11–1. Authentication Flowchart for Wireless Network Users**




## Summary of AAA Features

Depending on your network configuration, you can configure authentication, authorization, and accounting (AAA) for network users to be performed locally on the MX or remotely on a RADIUS server. The number of users that the local MX database can support depends on the MX model.

AAA for network users controls and monitors their use of the network:

- **Classification for customized access**. As with administrative and console users, you can classify network users through username globbing. Based on the structured username, different AAA types can be assigned to different classes of user. For example, users in the human resources department can be authenticated differently from users in the sales department.
- **Authentication for full or limited access.** IEEE 802.1X network users are authenticated when they identify themselves with a credential. Authentication can be passed through to RADIUS, performed locally on the MX, or only partially "offloaded" to the MX. Network users without 802.1X support can be authenticated by the MAC addresses of their devices. If neither 802.1X nor MAC authentication apply to the user, they can still be authenticated by a fallthru authentication type, either WebAAA or last-resort authentication. The default fallthru type is , which denies access to users that do not match an 802.1X or MAC authentication rule.

- **Authorization for access control**. Authorization provides access control by per-user security access control lists (ACLs), VLAN membership, Mobility Domain assignment, and timeout enforcement. Because authorization is always performed on users accessing a particular VLAN, the MX automatically uses the same AAA method (RADIUS server group or local database) for authorization that you define for a user authentication.
- **Local authorization control**. You can override any AAA assignment of VLAN or security ACL for individual network users on a particular MX by configuring the location policy on the MX.
- **SSID default authorization attributes**. You can configure service profiles with a set of default AAA authorization attributes that are applied when the normal AAA process or a location policy does not provide them.
- **Accounting for tracking users and resources**. Accounting collects and sends information used for billing, auditing, and reporting—for example, user identities, connection start and stop times, the number of packets received and sent, and the number of bytes transferred. You can track sessions by using accounting information stored locally or on a remote RADIUS server. As network users roam throughout a Mobility Domain, accounting records track them and their network usage.
- Accounting for administrative access sessions—Accounting records can be stored and displayed locally or sent to a RADIUS server. Accounting records provide an audit trail of the number of administrative logins, administrator username, number of bytes transferred, and the start and stop time of user sessions.

## AAA Tools for Network Users

Authentication verifies network user identity and is required before granting access to the network. An MX authenticates user identity by username-password matching, digital signatures and certificates, or other methods such as MAC addresses.

You must decide whether to authenticate network users locally on the MX, remotely via one or more external RADIUS server groups, or both locally and remotely.

## “Globs” and Groups for Network and Local User Classification

“Globbing” lets you classify users by username or MAC address for different AAA treatments. A user glob is a string used by AAA and IEEE 802.1X or WebAAA methods to match a user or set of users. MAC address globs match authentication methods to a MAC address or set of MAC addresses. User globs and MAC address globs can make use of wildcards. A user group is a named collection of users or MAC addresses sharing a common authorization policy. For example, you might group all users on the first floor of building 17 into the group bldg-17-1st-floor, or group all users in the IT group into the group infotech-people.

### Wildcard “Any” for SSID Matching

Authentication rules for wireless access include the SSID name, and must match the user-requested SSID name to authenticate the user for that SSID. To have an authentication rule match an any SSID string, specify the SSID name as any in the rule.

## Configuring the SSID Name “Any”

In authentication rules for wireless access, you can specify the name for the SSID. This value is a wildcard that matches any SSID string requested by the user.

For 802.1X and WebAAA rules that match on SSID , MSS checks the RADIUS servers or local database for the username (and password, if applicable) entered by the user. If the user information matches, MSS grants access to the SSID requested by the user, regardless of the SSID name.

For MAC authentication rules that match on SSID , MSS checks the RADIUS servers or local database for the MAC address (and password, if applicable) of the user device. If the address matches, MSS grants access to the SSID requested by the user, regardless of the SSID name.

## About Last-Resort Processing

One of the fallthru authentication types you can set on a service profile or wired authentication port is **last-resort**.

If no 802.1X or MAC access rules are configured for a service profile SSID, and the SSID fallthru type is **last-resort**, MSS allows users onto the SSID or port without prompting for a username or password. The default authorization attributes set on the SSID are applied to the user. For example, if the vlan-name attribute on the service profile is set to , last-resort users are placed in .

If no 802.1X or MAC access rules are configured for **wired**, and the wired authentication port fallthru type is **last-resort**, MSS allows users on the port without prompting for a username or password. The authorization attributes set on user are applied to the user.

depending on the type of authentication rule assigned to the SSID or wired access requested by the user.

- For a user to be successfully authenticated by an 802.1X or WebAAA rule, the username and password entered by the user must be configured on the RADIUS servers or in the local database.
- For a user to be successfully authenticated by a MAC address, the MAC address must be configured on the RADIUS servers used by the authentication rule or in the MX local database. If the MAC address is configured in the local database, no password is required. However, since RADIUS requires a password, if the MAC address is on the RADIUS server, MSS checks for a password. The default password is but is configurable.
- For a user to be successfully authenticated for last-resort access on a wired authentication port, the RADIUS servers or local database must contain a user named . If the user is configured in the local database, no password is required. However, since RADIUS requires a password, if the user is on the RADIUS server, MSS checks for a password. The default password is but is configurable.
- Last-resort access to an SSID does not require a special user (such as ***ssid***) to be configured. Instead, if the fallthru authentication type on the SSID service profile is set to **last-resort**, and the SSID does not have any 802.1X or MAC access rules, a user can access the SSID without entering a username or password.

## Authorization

If the user is authenticated, MSS then checks the RADIUS server or local database for the authorization attributes assigned to the user. Authorization attributes specify the network resources available to the user.

The Virtual LAN (VLAN) name is a required attribute in order to place the user in the appropriate network. RADIUS and MSS have additional optional attributes. For example, you can provide

MSS provides the following VSAs, that you can assign to users in the local database or on a RADIUS server:

- Encryption-Type—Specifies the type of encryption required for access by the client.
-

## AAA Rollover Process

An MX attempts AAA methods in the order that they are entered in the configuration:

1. The first AAA method in the list is used unless that method results in an error. If the method results in a pass or fail, the result is final and the MX tries no other methods.
2. If the MX receives no response from the first AAA method, the MX tries the second method in the list.
3. If the MX receives no response from the second AAA method, the MX tries the third method. This evaluation process is applied to all methods in the list.

## Local Override Exception

There is one exception to the AAA operation that takes place if the local database is the

## IEEE 802.1X Extensible Authentication Protocol Types

Extensible Authentication Protocol (EAP) is a generic point-to-point protocol that supports multiple authentication mechanisms. EAP has been adopted as a standard by the Institute of Electrical and Electronic Engineers (IEEE). IEEE 802.1X is an encapsulated form for carrying authentication messages in a standard message exchange between a user (client) and an authenticator.

**Table 11– 1** summarizes the EAP protocols supported by MSS.

## Implementing EAP on an MX

Network users with 802.1X support cannot access the network unless  authenticated. You can configure an MX to authenticate users with EAP on a group of RADIUS servers or in a local user database on the MX, or to offload some authentication tasks from the server group. **Table 11– 2** details these three basic MX authentication approaches.

## Configuring EAP Offload

You can configure the MX to offload all EAP processing from server groups. In this case, the RADIUS server is not required to communicate using the EAP protocols.

For PEAP-MS-CHAP-V2 offload, you define a complete user profile in the local MX database and only a username and password on a RADIUS server.

For example, the following command authenticates all wireless users who request SSID at example.com by offloading PEAP processing onto the MX, while still performing MS-CHAP-V2 authentication via the server group :

```
MX# set authentication dot1x ssid marshes *@example.com peap-mschapv2 shorebirds
```

To offload PEAP and MS-CHAP-V2 processing onto the MX, use the following command:

```
MX# set authentication dot1x ssid marshes *@example.com peap-mschapv2 local
```

## Using Pass-Through

The pass-through method causes EAP authentication requests to be processed entirely by remote RADIUS servers in server groups.

For example, the following command enables users at EXAMPLE to be processed via server group or :

```
MX# set authentication dot1X ssid marshes EXAMPLE/* pass-through shorebirds swamp-
    birds
```

The server group is contacted only if all the RADIUS servers in do not respond.

## Authenticating Users in a Local Database

To configure the MX to authenticate and authorize a user against the local database in the MX, use the following command:

```
set authentication dot1x {ssid ssid-name | wired} user-glob [bonded] protocol local
```

For example, the following command authenticates 802.1X user for wired authentication access via the local database:

```
MX-20# set authentication dot1X user wired peap-mschapv2 local
success: change accept 029.96 104.1 339.36 hapv2 l-sC6 hapvoio 0008  c.0008(ur74.2(ta1only)4.3
```

When Bonded Auth is enabled, MSS retains information about the computer session when a user logs on from that computer. MSS authenticates the user only if there has already been a successful computer authentication. Evidence of the computer session in MSS indicates that the computer has successfully authenticated and is therefore trusted by MSS. If MSS does not have session information for the computer, MSS refuses to authenticate the user and does not allow the user onto the network from the unauthenticated computer.


## Authentication Rule Requirements

Bonded Auth requires an 802.1X authentication rule for the computer, and a separate 802.1X authentication rule for the user(s). Use the **bonded** option in the user authentication rule, but not in the computer authentication rule.

The computer authentication rule must be higher in the list of authentication rules than the user authentication rule.

You must use 802.1X authentication rules. The computer 802.1X authentication rule must use **pass-through** as the protocol. Trapeze Networks recommends that you also use **pass-through** for the user authentication rule.

The computer rule and the user rule must use a RADIUS server group as the method. (Generally, in a Bonded Auth configuration, the RADIUS servers use a user database stored on an Active Directory server.)

(For a configuration example, see **"Bonded Authentication Configuration Example" on page 11–13**.)

It is recommended to make the rules as general as possible. For example, if the Active Directory domain is mycorp.com, the following userglobs match on all machine names and users in the domain:

- host/*.mycorp.com (userglob for the machine authentication rule)
- *.mycorp.com (userglob for the user authentication rule)

If the domain name has more nodes (for example, nl.mycorp.com), use an asterisk in each node that you want to match globally. For example, to match on all machines and users in mycorp.com, use the following userglobs:

- host/*.*.mycorp.com (userglob for the computer authentication rule)
- *.*.mycorp.com (userglob for the user authentication rule)

Use more specific rules to direct computers and users to different server groups. For example, to direct users in nl.mycorp.com to a different server group than users in de.mycorp.com, use the following userglobs:

- host/*.nl.mycorp.com (userglob for the computer authentication rule)
- *.nl.mycorp.com (userglob for the user authentication rule)
- host/*.de.mycorp.com (userglob for the computer authentication rule)
- *.de.mycorp.com (userglob for the user authentication rule)

## Bonded Authentication Period

The is the number of seconds MSS allows a Bonded Auth user to reauthenticate.

After successful computer authentication, a session appears in the session table in MSS. When the user logs on and is authenticated, the user session replaces the computer session in the table. However, since the user authentication rule contains the **bonded** option, MSS remembers that the computer was authenticated.

If a Bonded Authentication user session is ended due to 802.1X reauthentication or the RADIUS Session-Timeout parameter, MSS can allow time for the user to reauthenticate. The amount of time that MSS allows for reauthentication is controlled by the Bonded Authentication period.

If the user does not reauthenticate within the Bonded Authentication period, MSS deletes the information about the computer session. After the computer session information is deleted, the Bonded Authentication user cannot reauthenticate. When this occurs, the user must log off, and then log back on, to access the network. After multiple failed reauthentication attempts, the user might need to reboot the computer before logging on.

By default, the Bonded Authentication period is 0 seconds. MSS does not wait for a Bonded Authentication user to reauthenticate.

You can set the Bonded Authentication period to a value up to 300 seconds. Trapeze Networks recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

To set the Bonded Authentication period, use the following command:

```
set dot1x bonded-period seconds
```

To reset the Bonded Authentication period to the default value (0), use the following command:

```
clear dot1x bonded-period
```

## Bonded Authentication Configuration Example

To configure Bonded Authentication:

- Configure separate authentication rules for the computer and for the user(s).
- Set the Bonded Authentication period.
- Verify the configuration changes.

The following commands configure two 802.1X authentication rules for access to SSID . The first rule is for authentication of all trusted laptops at mycorp.com (host/*-laptop.mycorp.com). The second rule is for bonded authentication of all users at mycorp.com (*.mycorp.com). Both rules use pass-through as the protocol, and use RADIUS server group .

```
MX# set authentication dot1x ssid mycorp host/*-laptop.mycorp.com pass-through
        radgrp1
success: change accepted.
MX# set authentication dot1x ssid mycorp *.mycorp.com bonded pass-through radgrp1
success: change accepted.
```

The following command sets the Bonded Authentication period to 60 seconds, to allow time for WEP users to reauthenticate:

```
MX# set dot1x bonded-period 60
success: change accepted.
```

## Adding MAC Users and Groups

To create a MAC user group in the local MX database, you must associate it with an authorization attribute and value. Use the following command:

```
set mac-usergroup group-name attr attribute-name value
```

For example, to create a MAC user group called with a 3000-second Session-Timeout value, type the following command:

```
MX# set mac-usergroup mac-easters attr session-timeout 3000
success: change accepted.
```

To configure a MAC user in the local database and optionally add the user to a group, use the following command:

```
set mac-user mac-addr [group group-name]
```

```
success: change accepted
```

You can add authorization attributes to authenticated MAC users with the following command:

```
set mac-user mac-addr attr attribute-name value
```

For example, to add the MAC user 00:01:02:03:04:05 to VLAN :

```
MX# set mac-user 00:01:02:03:04:05 attr vlan-name red
success: change accepted
```

To change the value of an authorization attribute, reenter the command with the new value. To clear an authorization attribute from a MAC user profile in the local database, use the following command:

```
clear mac-user mac-addr attr attribute-name
```

For example, the following command clears the VLAN assignment from MAC user 01:0f:02:03:04:05:

```
MX# clear mac-user 01:0f:03:04:05:06 attr vlan-name
success: change accepted.
```

(For a complete list of authorization attributes, see Table 11– 5 on page 34.)

### Changing the MAC Authorization Password for RADIUS

To authenticate and authorize MAC users using RADIUS, you must configure a single predefined password for MAC users, called the outbound authorization password. The same password is used for all MAC user entries in the RADIUS database. Set this password by typing the following command:

```
set radius server server-name author-password password
```

The default password is .


Before setting the outbound authorization password for a RADIUS server, you must set the address for the RADIUS server.

For example, the following command sets the outbound authorization password for MAC users on server to :

```
MX# set radius server bigbird author-password h00per
success: change accepted.
```


If the MAC address is in the database, MSS uses the VLAN attribute and other attributes associated with it for user authorization. Otherwise, MSS tries the fallthru authentication type, which can be last-resort, Web, or none.

## Configuring Web Portal WebAAA

WebAAA provides a simple and universal way to authenticate any user or device using a Web browser. A common application of WebAAA is to control access for guests on your network. When a user requests access to an SSID or attempts to access a Web page before logging onto the network, MSS displays a login page to the user's browser. After the user enters a username and password, MSS validates the user information on the local database or RADIUS servers and grants or denies access based on whether the user information is found.

MSS redirects an authenticated user back to the requested web page, or to a page specified by the administrator.

WebAAA, like other types of authentication, is based on an SSID or on a wired authentication port.

You can use WebAAA on both encrypted and unencrypted SSIDs. If you use WebAAA on an encrypted SSID, you can use static WEP or WPA with PSK as the encryption type.

MSS provides a default Trapeze Networks login page but you can add custom login pages to the MX nonvolatile storage, and configure MSS to display these pages instead.

## How Web Portal WebAAA Works

1. A WebAAA user attempts to access the network. For a wireless user, this begins when the network interface card (NIC) associates with an SSID from a Trapeze MP. For a wired authentication user, this begins when the user NIC sends data on the wired authentication port.
2. MSS starts a portal session for the user, and places the user in a VLAN.
   - If the user is wireless (associated with an SSID), MSS assigns the user to the VLAN set by

### Display of the Login Page

When a WebAAA client first tries to access a Web page, the client browser sends a DNS request to obtain the IP address mapped to the domain name requested by the client browser. The MX proxies this DNS request to the network DNS server, then proxies the reply back to the client. If the DNS server has a record for the requested URL, the request is successful and the MX displays a Web login page to the client. However, if the DNS request is unsuccessful, the MX displays a message informing the user and does not serve the login page.

If the MX does not receive a reply to a client DNS request, the MX spoofs a reply to the browser by sending the MX IP address as the resolution to the browser DNS query. The MX also serves the Web login page. This behavior simplifies use of the WebAAA feature in networks that do not have a DNS server. However, if the requested URL is invalid, the behavior gives the appearance that the requested URL is valid, since the browser receives a login page. Moreover, the browser might cache a mapping of the invalid URL to the MX IP address.

If the user enters an IP address, most browsers attempt to contact the IP address directly without using DNS. Some browsers interpret numeric strings as IP addresses (in decimal notation) if a valid address could be formed by adding dots (dotted decimal notation). For example, 208194225132 would be interpreted as a valid IP address, when converted to 208.194.225.132.

## WebAAA Requirements and Recommendations

### MX Requirements

- WebAAA certificate—A WebAAA certificate must be installed on the MX. You can use a self-signed (signed by the MX) WebAAA certificate automatically generated by MSS, manually generate a self-signed one, or install one signed by a trusted third-party certificate authority (CA).

  If you decide to install a self-signed WebAAA certificate, use a common name (a required field in the certificate), that resembles a Web address and contains at least one dot. When MSS displays the login page in the Web browser, the page URL is based on the common name in the WebAAA certificate.

  Here are some examples of common names in the recommended format:

  - 

- Fallthru authentication type—The fallthru authentication type for each SSID and wired authentication port supporting WebAAA, must be set to **web-portal**. The default authentication type for wired authentication ports and for SSIDs is None (no fallthru authentication is used).

  To set the fallthru authentication type for an SSID, use the **set service-profile auth-fallthru** command. To set it on a wired authentication port, use the **auth-fall-thru web-portal** parameter of the **set port type wired-auth** command.

- Authorization attributes—Wireless Web-Portal users get their authorization attributes from the SSID service profile. To assign wireless Web-Portal users to a VLAN, use the **set service-profile attr vlan-name** command.

  Web-Portal users on wired authentication ports get their authorization attributes from the special user **web-portal-wired**. To assign wired Web-Portal users to a VLAN, use the **set user web-portal-wired attr vlan-name** command. By default, **web-portal-wired** users are assigned to the default VLAN.

- Portal ACL (created by MSS automatically)— The ACL captures all the portal user traffic except for DHCP traffic. The has the following ACEs:

```
set security acl ip portalacl permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0
        255.255.255.255 eq 67
set security acl ip portalacl deny 0.0.0.0 255.255.255.255 capture
```

  MSS automatically creates the ACL the first time you set the fallthru authentication type on any service profile or wired authentication port to **web-portal**.

  - The ACL is mapped to wireless Web-Portal users through the service profile. When you set the fallthru authentication type on a service profile to **web-portal**, is set as the Web-Portal ACL. The ACL is applied to a Web-Portal user traffic when the user associates with the service profile SSID.
  - The ACL is mapped to Web-Portal users on a wired-authentication port by the Filter-id.in attribute configured on the web-portal-wired user. When you set the fallthru authentication type on a wired authentication port to **web-portal**, MSS creates the **web-portal-wired** user. MSS sets the **filter-id** attribute on the user to **.in**.

- Authentication rules—A Wæn2(e)9.5904 0 1TD.0021 Tc-.0ypen rules.2(A.5(he)-5.9(td on916 0 TD951815 T

### Portal ACL and User ACLs

The ACL, which MSS creates automatically, applies only when a user session is in the portal state. After the user is authenticated and authorized, the ACL is no longer applicable.

3. Configure Web authentication rules for the WebAAA users.
4. Save the configuration changes.

## Web Portal WebAAA Configuration Example

This example configures Web-Portal access to SSID

4. Configure individual WebAAA users.

```
MX# set user alice password alicepword
success: change accepted.
MX# set user bob password bobpword
success: change accepted.
```

5. Configure a Web authentication rule for WebAAA users. The following rule uses a wildcard (**) to match on all user names.

   The ** value makes all usernames eligible for authentication. In this case by searching the local database on the MX for the matching usernames and passwords. If a username does not match on the access rule userglob, the user is denied access without searching the local database for the username and password.

```
MX# set authentication web ssid mycorp ** local
success: change accepted.
```

6. Display the configuration:

```
MX# show config
# Configuration nvgen'd at 2006-6-13 13:27:07
# Image 5.0.0.0.62
# Model MXR-2
# Last change occurred at 2006-6-13 13:24:46
...
set service-profile mycorp-srvcprof ssid-name mycorp
set service-profile mycorp-srvcprof auth-fallthru web-portal
set service-profile mycorp-srvcprof rsn-ie enable
set service-profile mycorp-srvcprof cipher-ccmp enable
set service-profile mycorp-srvcprof web-portal-acl portalacl
set service-profile mycorp-srvcprof attr vlan-name mycorp-vlan
...
set authentication web ssid mycorp ** local
...
set user alice password encrypted 070e2d454d0c091218000f
set user bob password encrypted 110b16070705041e00
...
set radio-profile radprof1 service-profile mycorp-srvcprof
set ap 7 radio 2 radio-profile radprof1 mode enable
set ap 8 radio 2 radio-profile radprof1 mode enable
...
set vlan corpvlan port 2-3
set interface corpvlan ip 192.168.12.10 255.255.255.0
...
set security acl ip portalacl permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0
        255.255.255.255 eq 67
set security acl ip portalacl deny 0.0.0.0 255.255.255.255 capture
commit security acl portalacl
```

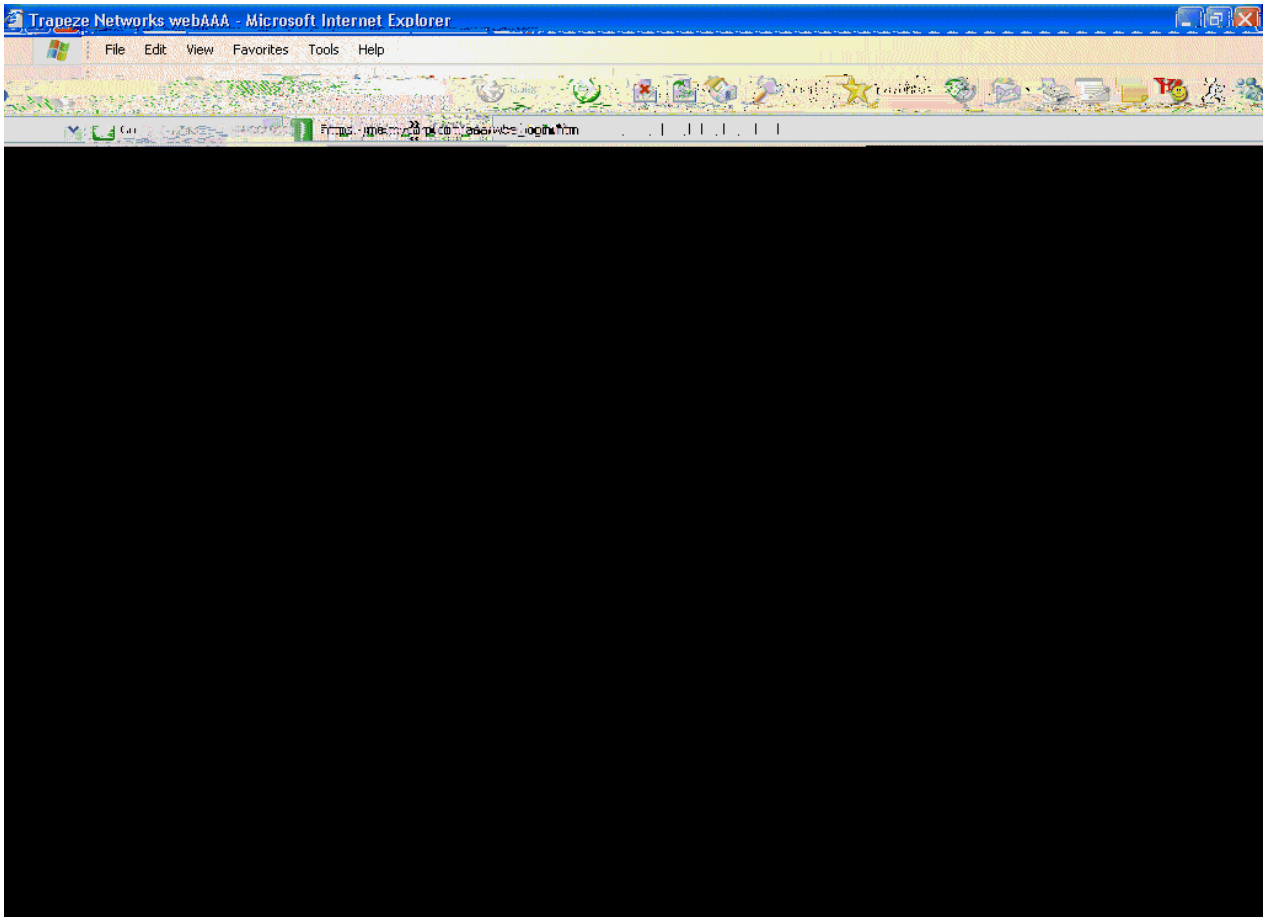
## External Captive Portal Support

The ability to redirect Web portal authentication to a Web server on a network rather than a local MX database or RADIUS is now available in MSS 7.0. The feature works in the following manner:

❑

## Using a Custom Login Page

By default, MSS displays the Trapeze Networks login page for Web login.




MSS uses the following process to locate the login page to display to a user:

- If the user is attempting to access an SSID and a custom page is specified in the service profile, MSS serves the custom page.
- If the MX nonvolatile storage has a page in named ( ), MSS serves this page. This applies to all wired authentication users. The page also is served to SSID users if the SSID service profile does not specify a custom page.
- If there is no page and no custom page in the service profile of an SSID, MSS serves the default page.

### Copying and Modifying the Web Login Page

To copy and modify the Trapeze Web login page:

1. Configure an unencrypted SSID on an MX. The SSID is temporary and does not need to be one you intend to use in your network. To configure the SSID, use the following commands:

```
set service-profile name ssid-name ssid-name
set service-profile name ssid-type clear
set service-profile name auth-fallthru web-portal
set radio-profile name service-profile name
set ap apnum radio {1 | 2} radio-profile name mode enable
```

Use the first two commands to configure a te

```
<h3>Welcome to Mycorp's Wireless LAN</h3>
```

**d.** Change the warning statement if desired:

```
<b>WARNING:</b>
My corp's warning text.
```

***e.***

6. Save the modified page.
7. On the MX, create a new subdirectory for the customized page. (The files must be on a TFTP server that the MX can access over the network.)

```
MX# mkdir mycorp-webaaa
success: change accepted.
```

8. Copy the files for the customized page

## Using Dynamic Fields in WebAAA Redirect URLs

You can include variables in the URL to redirect a WebAAA client. **Table 11– 3** lists the variables you can include in a redirect URL.

A URL string can also contain the literal characters $ and ?, if you use the values listed in **Table 11– 4**.

You can configure a redirect URL for a group of users or for an individual user. For example, the following command configures

## Using an ACL Other Than *portalacl*

By default, when you set the fallthru authentication type on a service profile or wired authentication port to **web-portal**, MSS creates an ACL called . MSS uses the ACL to filter Web-Portal user traffic while users are authenticating.

To use another ACL:

1. Create a new ACL and add the first rule contained in :

```
set security acl ip portalacl permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0
        255.255.255.255 eq 67
set security acl ip portalacl deny 0.0.0.0 255.255.255.255 capture
```

2. Add the additional rules required for your application. For example, if you want to redirect users to a credit card server, add the necessary ACEs.
3. Add the last rule contained in :

```
set security acl ip portalacl deny 0.0.0.0 255.255.255.255 capture
```

4. Verify the new ACL configuration, before committing it, using the following command:

```
show security acl info [acl-name | all] [editbuffer]
```

5. Commit the new ACL to the configuration, using the following command:

```
commit security acl
```

6. Change the Web-Portal ACL name set on the service profile, using the following command:

```
set service-profile name web-portal-acl aclname
```

7. Verify the change by displaying the service profile.
8. Save the configuration changes.

## Configuring the Web Portal WebAAA Session Timeout Period

When a client that has connected through Web Portal, WebAAA enters standby or hibernation mode, and MSS may place the Web Portal WebAAA client session in the state.

A Web Portal WebAAA session can be placed in the Disassociated state under the following circumstances:

- The client has been idle for the User idle-timeout period.
- The client explicitly deassociates from the MP by sending an 802.11 disassociate message
- The MP handling the client session appears to be inoperative from the MX.

When a Web Portal WebAAA session

The authentication method for last-resort is always local. MSS does not use RADIUS for last-resort authentication.

The following commands configure last-resort access for SSID . The service profile is configured to encrypt user traffic on the SSID using 40-bit dynamic WEP, WPA, or RSN, depending on the client configuration.

```
MX# set service-profile last-resort-srvcprof ssid-name guest-wlan
success: change accepted.
MX# set service-profile last-resort-srvcprof auth-fallthru last-resort
success: change accepted.
MX# set service-profile last-resort-srvcprof attr vlan-name guest-vlan
success: change accepted.
MX# set service-profile last-resort-srvcprof rsn-ie enable
success: change accepted.
MX# set service-profile last-resort-srvcprof wpa-ie enable
success: change accepted.
MX# set service-profile last-resort-srvcprof cipher-ccmp enable
success: change accepted.
MX2# set service-profile last-resort-srvcprof cipher-wep40 enable
success: change accepted.
MX# show service-profile last-resort-srvcprof
ssid-name:                  guest-wlan   ssid-type:                        crypto
Beacon:                            yes   Proxy ARP:                           no
DHCP restrict:                      no   No broadcast:                        no
Short retry limit:                   5   Long retry limit:                     5
Auth fallthru:              last-resort   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
CAC mode:                         none   CAC sessions:                        14
 ser idle timeout:                 180   Idle client probing:                yes
Keep initial vlan:                  no   Web Portal Session  imeout:           5
Web Portal ACL:
WEP Key 1 value:                <none>   WEP Key 2 value:                  <none>
WEP Key 3 value:                <none>   WEP Key 4 value:                  <none>
WEP  nicast Index:                   1   WEP Multicast Index:                  1
Shared Key Auth:                    NO
WPA and RSN enabled:
    ciphers: cipher-tkip, cipher-ccmp, cipher-wep40
    authentication: 802.1X
     KIP countermeasures time: 60000ms
vlan-name = guest-vlan
...
```

## Configuring Last-Resort Access for Wired Authentication Ports

To configure a wired authentication port to allow last-resort access:

- Set the fallthru authentication type on the port to **last-resort**.
- Create a user named last-resort-wired in the MX local database.

The following commands configure wired authentication port 5 for last-resort access and add the special user:

```
success: change accepted.
MX#uD[( se)6.9(d l succ)6o t sera  Idl gt serrt
```

# Configuring AAA for Users of Third-Party APs

An MX can provide network access for users associated with a third-party AP that has authenticated the users with RADIUS. You can connect a third-party AP to an MX and configure the MX to provide authorization for clients who authenticate and access the network through the AP. **Figure 11–3** shows an example.

**Figure 11–3. MX Serving as RADIUS Proxy**

## Authentication Process for Users of a Third-Party AP

1. MSS uses MAC authentication to authenticate the AP.
2. The user contacts the AP and negotiates the authentication protocol.
3. The AP, acting as a RADIUS client, sends a RADIUS access-request to the MX. The access-request includes the SSID, the user MAC address, and the username.
4. For 802.1X users, the AP uses 802.1X to authenticate the user, using the MX as its RADIUS server. The MX proxies RADIUS requests from the AP to a RADIUS server, depending on the authentication method specified in the user proxy authentication rule.
5.

## MX Requirements

- The MX port connected to the third-party AP must be configured as a wired authentication port. If SSID traffic from the AP is tagged, the same VLAN tag value must be used on the wired authentication port.
- A MAC authentication rule must be configured to authenticate the AP.
-

For the of the **set radius proxy client address** command, specify the IP address of the RADIUS client (the third-party AP). For the , specify the UDP port on which the MX listens for RADIUS access-requests. The default is UDP port 1812. For the , specify the UDP port on which the MX listens for RADIUS stop-accounting records. The default is UDP port 1813.

The following command configures MX ports 3 and 4 as wired authentication ports, and assigns tag value 104 to the ports:

```
MX# set port type wired-auth 3-4 tag 104
success: change accepted.
```

You can specify multiple tag values. Specify the tag value for each SSID you plan to support.

The following command configures a MAC authentication rule that matches on the third-party AP MAC address. Because the AP is connected to the MX on a wired authentication port, the **wired** option is used.

```
MX# set authentication mac wired aa:bb:cc:01:01:01 srvrgrp1
success: change accepted.
```

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.
```

Enter a separate command for each SSID, and the tag value supported by the MX.

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.
```

The IP address is the IP address of the AP. The key is the shared secret configured on the RADIUS servers. MSS uses the shared secret to authenticate and encrypt RADIUS communication.

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
```

To verify the changes, use the **show config area aaa** command.

## Configuring Authentication — Non-802.1X Users of a Third-Party AP, Tagged SSIDs

To configure MSS to authenticate non-802.1X users of a third-party AP, use the same commands as those required for 802.1X users. Additionally, when configuring the wired authentication port, use the **auth-fall-thru** option to change the fallthru authentication type to **last-resort** or **web-portal**.

### Configuring Access for Any Users of a Non-Tagged SSID

If SSID traffic from the third-party AP is untagged, use the same configuration commands as the ones required for 802.1X users, except the **set radius proxy port** command. This command is not required and is not applicable to untagged SSID traffic. In addition, when configuring the wired authentication port, use the **auth-fall-thru** option to change the fallthru authentication type to **last-resort** or **web-portal**.

On the RADIUS server, configure the username **web-portal-wired** or **last-resort-wired**, depending on the fallthru authentication type specified for the wired authentication port.

## Assigning Authorization Attributes

Authorization attributes can be assigned to users in the local database, on remote servers, or in the service profile of an SSID. The attributes, which include access control list (ACL) filters, VLAN membership, encryption type, session time-out period, and other session characteristics, let you control how and when users access the network. When a user or group is authenticated, the local database, RADIUS server, or service profile passes the authorization attributes to MSS to characterize the user session.

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

The VLAN attribute is required. A user can access the network only if the user VLAN is specified.

**Table 11– 5** lists the authorization attributes supported by MSS. (For brief descriptions of all the RADIUS attributes and Trapeze vendor-specific attributes supported by MSS, as well as the vendor ID and types for Trapeze VSAs configured on a RADIUS server, see the .)

**Table 11– 5. Authentication Attributes for Local Users**

| Attribute | Description | Valid Value(s) |
|---|---|---|
| **encryption-type** | Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected. | |

| | |
|---|---|
| **filter-id** (network access mode only) | Security access control list (ACL), to permit or deny traffic received (input) or sent (output) by the MX switch. (For more information about security ACLs, see Chapter 24, |

| | | |
|---|---|---|
| | Date and time at which the user becomes eligible to access the network.<br>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:<br>YY/MM/DD-HH:MM<br>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**. |
| **y**<br>ccess mode | Day(s) and time(s) during which the user is permitted to log into the network.<br>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. | One of the following:<br>❑ **never**—Access is always denied.<br>❑ **any**—Access is always allowed.<br>❑ **al**—Access is always allowed.<br>❑ 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):<br>**mo**<br>**tu**<br>**we**<br>**th**<br>**fr**<br>**sa**<br>**su**<br>**wk**<br>Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (\|). Do not use spaces.<br>The maximum number of characters is 253.<br>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**<br>To allow access only on weekdays between 9 a.m and 5 p.m., and on Saturdays from 10 p.m. until 2 a.m., specify the following:<br>**time-of-day wk0900-1700,sa2200-0200**<br>**Note: time-of-day start-date end-date** |
| ccess mode | URL to which the user is redirected after successful WebAAA. | Web URL, in standard format. For example:<br>http://www.example.com<br>**Note:** |

If you set the attribute to 0, then the user is locked out of the network. The default value is unlimited access. In addition, setting this value applies only to user session in the mobility domain and not a specific MX. Additional commands include the following:

`MX200# set usergroup group attr simultaneous-logins 0-1000`

`MX200# set service-profile profile-name attr simultaneous-logins 0-1000`To clear the configuration, enter

`MX200# clear user username> attr simultaneous-logins`

## Assigning SSID Default Attributes to a Service Profile

You can configure a service profile with a set of default AAA authorization attributes used when the normal AAA process or a location policy does not provide them. These authorization attributes are applied by default to users accessing the SSID managed by the service profile.

Use the following command to assign an authorization attribute to a service profile and specify a value:

`set service-profile profile-name attr attribute-name value`

By default, a service profile contains no SSID default authorization attributes. When specified, attributes in a service profile 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

You can set filters for incoming and outgoing packets:

Clients attempting to use an unauthorized encryption method are rejected.

## Assigning and Clearing Encryption Types Locally

To restrict wireless uses or groups with user profiles in the local MX database to particular encryption algorithms for accessing the network, use one of the following commands:

```
set user username attr encryption-type value
set usergroup groupname attr encryption-type value
set mac-user username attr encryption-type value
set mac-user mac-glob attr value
set mac-usergroup groupname attr encryption-type value
```

MSS supports the following values for Encryption-Type, listed from most secure to least secure. (For user encryption details, see Chapter 15, “Configuring User Encryption,” on page 15-1.)

For example, the following command restricts the MAC user group to access the network by using only TKIP:

```
MX# set mac-usergroup mac-fans attr encryption-type 4
success: change accepted.
```

You can also specify a combination of allowed encryption types by adding the values together. For example, the following command allows to associate using either TKIP (4) or WEP_104 (8):

```
MX# set mac-usergroup mac-fans attr encryption-type 12
success: change accepted.
```

To clear an encryption type from the profile of a use or group of users in the local MX datav0 T Tm-. attD2 7 at23

## Keeping Users on the Same VLAN Even After Roaming

In some cases, a user is assigned to a different VLAN after roaming to another MX. **Table 11– 6** lists the ways a VLAN is assigned to a user after roaming from one MX to another.

**Table 11– 6. VLAN Assignment After Roaming from One MX to Another**

| Location Policy | AAA | keep-initial-vlan | SSID | VLAN Assigned By... |
|---|---|---|---|---|
| Yes | Yes or No | Yes or No | Yes or No | location policy |
| No | Yes | Yes or No | Yes or No | AAA |
| No | No | Yes | Yes or No | keep-initial-vlan |
| No | No | No | Yes | SSID |
| No | No | No | No | Not set— authentication error |

in the table means the VLAN is set on the roamed-to MX, by the mechanism indicated by the column header. means the VLAN is not set. means the mechanism does not affect the outcome, because another mechanism is set.

The column indicates the mechanism used by the roamed-to MX to assign the VLAN, based on the various ways the VLAN is set on that MX.

- means the VLAN is assigned by a location policy on the roamed-to MX. (The VLAN is assigned by the **vlan** option of the **set location policy permit** command.)
- means the Vlan-name attribute is set on for the user or the user group, in the roamed-to MX local database or on a RADIUS server used by the roamed-to MX to authenticate the user. (The VLAN is assigned by the **vlan-name** option of the **set user attr**, **set usergroup attr**, **set mac-user**, or **set mac-usergroup** command.)
- means that the VLAN is not reassigned. Instead, the VLAN assigned on the first MX is retained. (The **keep-initial-vlan** option is enabled by the **set service-profile keep-initial-vlan enable** command, entered on the roamed-to MX. The is the name of the service profile for the associated user SSID.)
- means the VLAN is set on the roamed-to MX, in the service profile for the associated user SSID. (The Vlan-name attribute is set by the **set service-profile attr vlan-name** command, entered on the roamed-to MX. The is the name of the service profile for the SSID the user is associated with.)
- As shown in **Table 11– 6**, even when **keep-initial-vlan** is set, a user VLAN can be reassigned by AAA or a location policy.

To enable **keep-initial-vlan**, use the following command:

```
set service-profile name keep-initial-vlan {enable | disable}
```

Enter this command on the MX configured for roaming by users.

The following command enables the **keep-initial-vlan** option on service profile :

```
MX# set service-profile sp3 keep-initial-vlan enable
success: change accepted.
```

# Overriding or Adding Attributes Locally with a Location Policy

During the login process, the AAA authorization process is started immediately after clients are authenticated on the MX. During authorization, MSS assigns the user to a VLAN and applies

You must specify whether to permit or deny access, and you must identify a VLAN, username, or access port to match. Use one of the following operators to specify how the rule must match the

```
Id Clauses
-----------------------------------------------------------------
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.ourfirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.ourfirm.com
4) permit inacl svcs_2.in outacl svcs_3.out if vlan eq bldg4.*
 o move the first rule to the end of the list and display the results, type the fol-
        lowing commands:
MX clear location policy 1
success: clause 1 is removed.
MX set location policy deny if user eq *.theirfirm.com
MX show location policy
Id Clauses
-----------------------------------------------------------------
1) permit vlan guest_1 if vlan neq *.ourfirm.com
2) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.ourfirm.com
3) permit inacl svcs_2.in outacl svcs_3.out if vlan eq bldg4.*
4) deny if user eq *.theirfirm.com
```

### Clearing Location Policy Rules and Disabling the Location Policy

To delete a location policy rule, use the following command:

```
clear location policy rule-number
```

Type **show location policy** to display the numbers of configured location policy rules. To disable the location policy on an MX, delete all the location policy rules.

## Configuring Accounting for Wireless Network Users

Accounting records come in three types: start, stop, and update. MSS generates these records based on the configured accounting 1sers

(For details about **show accounting statistics** output, see the
. For information about accounting update records, see

```
Acct-Multi-Session-Id=SESSION-4-1106424789
 ser-Name=Administrator@example.com
Acct-Session- ime=361
Event- imestamp=1053536852
Acct-Output-Octets=2560
Acct-Input-Octets=5760
Acct-Output-Packets=20
Acct-Input-Packets=45
Vlan-Name=default
Calling-Station-Id=00-06-25-09-39-5D
Nas-Port-Id=2/1
Called-Station-Id=00-0B-0E-76-56-A0
```

If you configured accounting records to be sent to a RADIUS server, you can view the records of user roaming at the RADIUS server. (For more information on these attributes, see the .)

For information about requesting accounting records from the RADIUS server, see the documentation for your RADIUS server.

# Displaying the AAA Configuration

To view the output of the configured AAA commands and verify the order, type the **show aaa** command. The order in which the commands appear in the output determines the order in which MSS matches them to users.

(Sometimes the order might not be what you intended. See **Avoiding AAA Problems in Configuration Order**.)

For example:

```
MX# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)
Radius Servers
Server                   Addr           Ports    /o  ries Dead State
-------------------------------------------------------------------
rs-3                 198.162.1.1     1821 1813  5    3    0     P
rs-4                 198.168.1.2     1821 1813  77   11   2     P
rs-5                 198.162.1.3     1821 1813  42   23   0     P
Server groups
sg1: rs-3
sg2: rs-4
sg3: rs-5

Web Portal:
enabled

set authentication admin Jose sg3
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set accounting dot1x Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local
user Nin
Password = 082c6c64060b (encrypted)
Filter-Id = acl-999.in
Filter-Id = acl-999.out
mac-user 01:02:03:04:05:06
usergroup eastcoasters
   session-timeout = 99
```

For information about the fields in the output, see the .

### Configuration for a Correct Processing Order

To avoid processing errors for authentication and accounting commands that include order-sensitive user globs, enter the commands for each user glob in pairs.

For example, to set accounting and authorization for 802.1X users as you intended, enter an accounting and authentication command for each user glob in the order in which you want them processed:

```
MX# set accounting dot1x ssid mycorp EXAMPLE/* start-stop group1
success: change accepted.
MX# set authentication dot1x ssid mycorp EXAMPLE/* peap-mschapv2 group1
success: change accepted.
MX# set accounting dot1x ssid mycorp * start-stop group1
success: change accepted.
MX# set authentication dot1x ssid mycorp * peap-mschapv2 local
success: change accepted.
```

The configuration order now shows that all 802.1X users are processed as you intended:

```
MX# show aaa
...
set accounting dot1x ssid mycorp EXAMPLE/* start-stop group1
set authentication dot1x ssid mycorp EXAMPLE/* peap-mschapv2 group1
set accounting dot1x ssid mycorp * start-stop group1
set authentication dot1x ssid mycorp * peap-mschapv2 local
```

## Configuring a Mobility Profile

A Mobility Profile is a way of specifying, on a per-user basis, those users allowed access to specified MP access ports and wired authentication ports on an MX. In this way, you can constrain the roaming areas for users. You first create a Mobility Profile, assign the profile to one or more users, and finally enable the Mobility Profile feature on the MX.

Use the following command to create a Mobility Profile by giving it a name and identifying the accessible port or ports:

```
set mobility-profile name name
        {port {none | all | port-list}} | {ap {none | all | apnum}
```

Specifying **none** prevents users assigned to the Mobility Profile from accessing any MP access ports, Distributed MPs, or wired authentication ports on the MX. Specifying **all** allows the users access to all of the ports or Distributed MPs.

Specifying an individual port or Distributed MP number or a list limits access to those ports or MPs. For example, the following command creates a Mobility Profile named that allows access through ports 2 through 4, port 7, and port 9:

```
MX# set mobility-profile name roses-profile port 2-4,7,9
success: change accepted.
```

You can then assign this Mobility Profile to one or more users. For example, to assign the Mobility Profile to all users at EXAMPLE\, type the following command:

```
MX# set user EXAMPLE\* attr mobility-profile roses-profile
success: change accepted.
```

During 802.1X authorization for clients at EXAMPLE\, MSS must search for the Mobility Profile named . If it is not found, the authorization fails and clients with usernames like EXAMPLE\jose and EXAMPLE\tamara are rejected.

If is configured for EXAMPLE\ users on your MX, MSS verifies the port list. If, for example, the current port for EXAMPLE\jose's connection is on the list of allowed ports specified in , the connection is allowed to proceed. If the port is not in the list (for example, EXAMPLE\jose is on port 12, which is not in the port list), the authorization fails and client EXAMPLE\jose is rejected.

The Mobility Profile feature is disabled by default. You must enable Mobility Profile attributes on the MX to use it. You can enable or disable the feature for the whole MX only. If the Mobility Profile feature is disabled, all Mobility Profile attributes are ignored.

To put Mobility Profile attributes into effect on an MX, type the following command:

```
MX# set mobility-profile mode enable
success: change accepted.
```

To display the name of each Mobility Profile and the ports, type the following command:

```
MX# show mobility-profile
Mobility Profiles
Name                Ports
=======================
roses-profile
                AP 2
                AP 3
                AP 4
                AP 7
                AP 9
```

To remove a Mobility Profile, type the following command:

```
clear mobility-profile name
```

# Network User Configuration Scenarios

The following scenarios provide examples of ways in which you use AAA commands to configure access for users:

- **"General Use of Network User Commands" on page 11–50**
- **"Enabling RADIUS Pass-Through Authentication" on page 11–51**
- **"Enabling PEAP-MS-CHAP-V2 Authentication" on page 11–52**
- **"Enabling PEAP-MS-CHAP-V2 Offload" on page 11–52**
- **"Combining EAP Offload with Pass-Through Authentication" on page 11–52**
- **"Overriding AAA-Assigned VLANs" on page 11–53**

## General Use of Network User Commands

The following example illustrates how to configure IEEE 802.1X network users for authentication, accounting, ACL filtering, and Mobility Profile assignment:

1. Configure all 802.1X users of SSID at EXAMPLE to be authenticated by server group Type the following command:

```
MX-20# set authentication dot1x ssid mycorp EXAMPLE\* pass-through shorebirds
```

2. Configure stop-only accounting for all users at EXAMPLE, for accounting records to be stored locally. Type the following command:

```
set security acl ip acl-101 (hits #0 0)
---------------------------------------------------
 1. permit IP source IP 192.168.1.1 0.0.0.255 destination IP any enable-hits
```

(For more information about ACLs, see Chapter 24, “Configuring and Managing Security ACLs,” on page 24-1.)

**5.** Create a Mobility Profile called by typing the following commands:

```
MX# set mobility-profile name tulip port 2,5-9
success: change accepted.
MX# set mobility-profile mode enable
success: change accepted.
MX# show mobility-profile
Mobility Profiles
Name                Ports
=========================
tulip
                  AP 2
                  AP 6
                  AP 7
                  AP 8
                  AP 9
```

**6.** To assign Mobility Profile to all users at EXAMPLE, type the following command for EXAMPLE\ user:

```
MX# set user EXAMPLE\username attr mobility-profile tulip
```

Users at EXAMPLE are now restricted to ports 2 and 5 through 9, as specified in the Mobility Profile configuration.

**7.** Use the **show aaa** command to verify your configuration. Type the following command:

```
MX# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)
Radius Servers
Server                  Addr           Ports    /o  ries Dead State
-------------------------------------------------------------------

Web Portal:
enabled

set accounting dot1x ssid mycorp EXAMPLE\* stop-only local
set authentication dot1x ssid mycorp EXAMPLE\* pass-through shorebirds
user tech
   Password = 1315021018 (encrypted)
user EXAMPLE/nin
   filter-id = acl.101.in
   mobility-profile = tulip
user EXAMPLE/tamara
   filter-id = acl.101.in
   mobility-profile = tulip
...
```

**8.** Save the configuration:

```
MX save config
success: configuration saved.
```

## Enabling RADIUS Pass-Through Authentication

The following example illustrates how to enable RADIUS pass-through authentication for all 802.1X network users:

**1.**

```
MX# set radius server r1 address 10.1.1.1 key sunny
```

2. Configure the server group with member . Type the following command:

```
MX# set server group sg1 members r1
```

3. Enable all 802.1X users of SSID to authenticate via pass-through to server group . Type the following command:

```
MX# set authentication dot1x ssid mycorp * pass-through sg1
```

4. Save the configuration:

```
MX save config
success: configuration saved.
```

## Enabling PEAP-MS-CHAP-V2 Authentication

The following example illustrates how to enable local PEAP-MS-CHAP-V2 authentication for all 802.1X network users. This example includes local usernames, passwords, and membership in a VLAN. This example includes one username and an optional attribute for session-timeout in seconds.

1. To set authentication for all 802.1X users of SSID , type the following command:

```
MX# set authentication dot1x ssid thiscorp * peap-mschapv2 local
```

2. To add user Natasha to the local database on the MX switch, type the following command:

```
MX# set user Natasha password moon
```

3. To assign Natasha to a VLAN named , type the following command:

```
MX# set user Natasha attr vlan-name red
```

4. To assign Natasha a session timeout value of 1200 seconds, type the following command:

```
MX# set user Natasha attr session-timeout 1200
```

5. Save the configuration:

```
MX save config
success: configuration saved.
```

## Enabling PEAP-MS-CHAP-V2 Offload

The following example illustrates how to enable PEAP-MS-CHAP-V2 offload. In this example, all EAP processing is offloaded from the RADIUS server, but MS-CHAP-V2 authentication and authorization are performed on a RADIUS server. The MS-CHAP-V2 lookup matches users against the user list on a RADIUS server.

1. Configure the RADIUS server at IP address 10.1.1.1 with the string for the key. Type the following command:

```
MX# set radius server r1 address 10.1.1.1 key starry
```

2. Configure the server group with member . Type the following command:

```
MX# set server group sg1 members r1
```

3. Enable all 802.1X users of SSID using PEAP-MS-CHAP-V2 to authenticate MS-CHAP-V2 on server group . Type the following command:

```
MX# set authentication dot1x ssid thiscorp * peap-mschapv2 sg1
```

4. Save the configuration:

```
MX save config
success: configuration saved.
```

## Combining EAP Offload with Pass-Through Authentication

The following example illustrates how to enable PEAP-MS-CHAP-V2 offload for the marketing ( ) group and RADIUS pass-through authentication for members of engineering. This example assumes that engineering members are using DNS-style naming, such as is used with EAP-TLS. An MX server certificate is also required.

1. Configure the RADIUS server at IP address 10.1.1.1 with the string for the key. Type the following command:

```
MX# set radius server r1 address 10.1.1.1 key starry
```

2. Configure the server group with member . Type the following command:

```
MX# set server group sg1 members r1
```

3. To authenticate all 802.1X users of SSID in the group using PEAP on the MX and MS-CHAP-V2 on server , type the following command:

```
MX# set authentication dot1x ssid bobblehead mktg\* peap-mschapv2 sg1
```

4. To authenticate all 802.1X users of SSID in @eng.example.com via pass-through to , type the following command:

```
MX# set authentication dot1x ssid aircorp *@eng.example.com pass-through sg1
```

5.

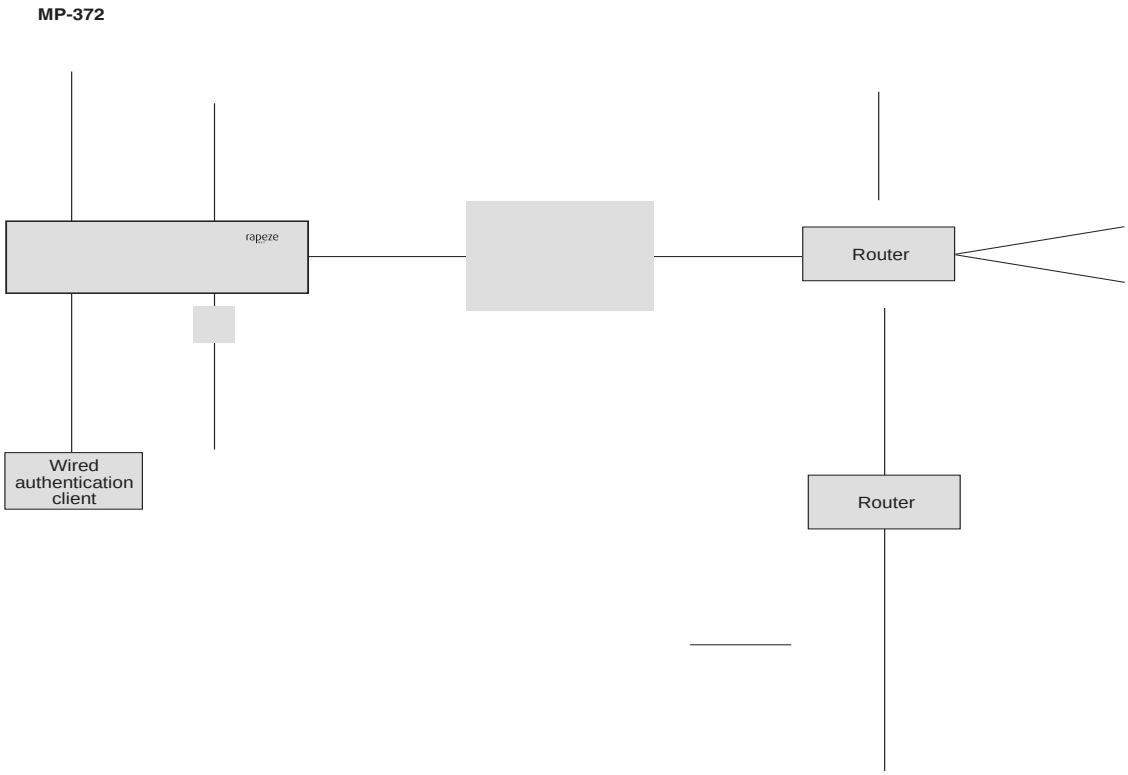
# Configuring Mobility Points

Mobility Points contain radios that provide connections between your wired network and IEEE 802.11 wireless users. An MP connects to the wired network through a 10/100 Ethernet link and connects to wireless users through radio signals.

## MP Overview

**Figure 12–1** shows an example of a Trapeze network containing MPs and MX switches. An MP can be directly connected to an MX port or indirectly connected to an MX through a Layer 2 or IPv4 Layer 3 network.

**Figure 12–1. Example of a Trapeze Network Topology**




To configure MP access points, perform the following tasks:

- Specify the country of operation.
- Configure MP access ports, Distributed MP connections, and dual homing.

- If required, configure radio-specific parameters, including the channel number, transmit power, and external antenna model (optional).

- Configure SSID and encryption settings in a service profile.
- Map the service profile to a radio profile.
- Assign the radio profile to radios, and enable the radios.

## Network Address Translation (NAT) Support

MSS supports network address translation (NAT) which provides the translation of IP addresses

- **DHCP**—By default, a Distributed MP uses TCP/IP for communication, and relies on DHCP to obtain IP information. Therefore, DHCP services must be available on the subnet connected to the MP. DHCP must provide the following parameters to the MP:
  - IP address
  - Domain name
  - DNS server address
  - Default router address
- **Static IP configuration**—If DHCP is not available in the network, a Distributed MP can be configured with static IP information and the MX to use as the boot device.
- **DNS**—If the intermediate network between the MX and Distributed MP includes one or more IP routers, create a TRPZ. .com or wlan-switch. .com entry on the DNS server. The entry needs to map one of these names to the system IP address of the MX. If the subnet contains more than one MX in the same Mobility Domain, you can use the system IP address of any of the MX switches. (For redundancy, you can create more than one DNS entry, and map each entry to a different MX in the subnet.)

  The DNS entry allows the MP to communicate with an MX not on the MP subnet. If the MP cannot locate an MX on the same subnet, the MP sends DNS requests to both and , and the DNS suffix for .com is obtained through DHCP.

- If only is defined in DNS, the MP contacts the MX with an IP address returned for .
- If only is defined in DNS, the MP contacts the MX with the IP address for .
- If both and are defined in DNS, the MP contacts the MX with IP address for . The MP ignores the IP address for .
- If both and are defined in DNS, and the MP is unable to contact the IP address for , the MP never contacts the IP address returned for . The MP does not boot.

## Distributed MPs and Spanning Tree Protocol (STP)

TRPZ

- If the other device is running Rapid Spanning Tree or Multiple Spanning Tree, configure the port for edge port mode.

## Distributed MPs and DHCP Option 43

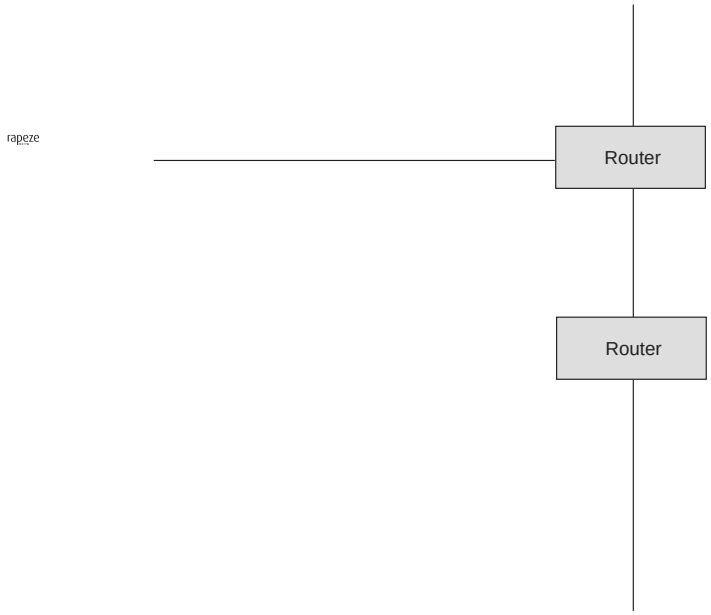
The option 43 field in a DHCP Offer message can provide a simple and effective way for MPs to find MX switches across an intermediate Layer 3 network. It is espe

- **Figure 12–4 on page 7** shows an example of the boot process for a dual-homed MP with one direct connection to an MX and an indirect connection through a Layer 2 network.
- **Figure 12–5 on page 8** shows an example of the boot process for an MP configured with static IP information.

### Example of an MP Booting over a Layer 2 Network

**Figure 12–2** shows an example of the boot process for an MP connected through a Layer 2 network. MX1, MX2, and MX3 each have a Distributed MP configuration for the MP.

**Figure 12–2. An MP Booting over a Layer 2 Network**



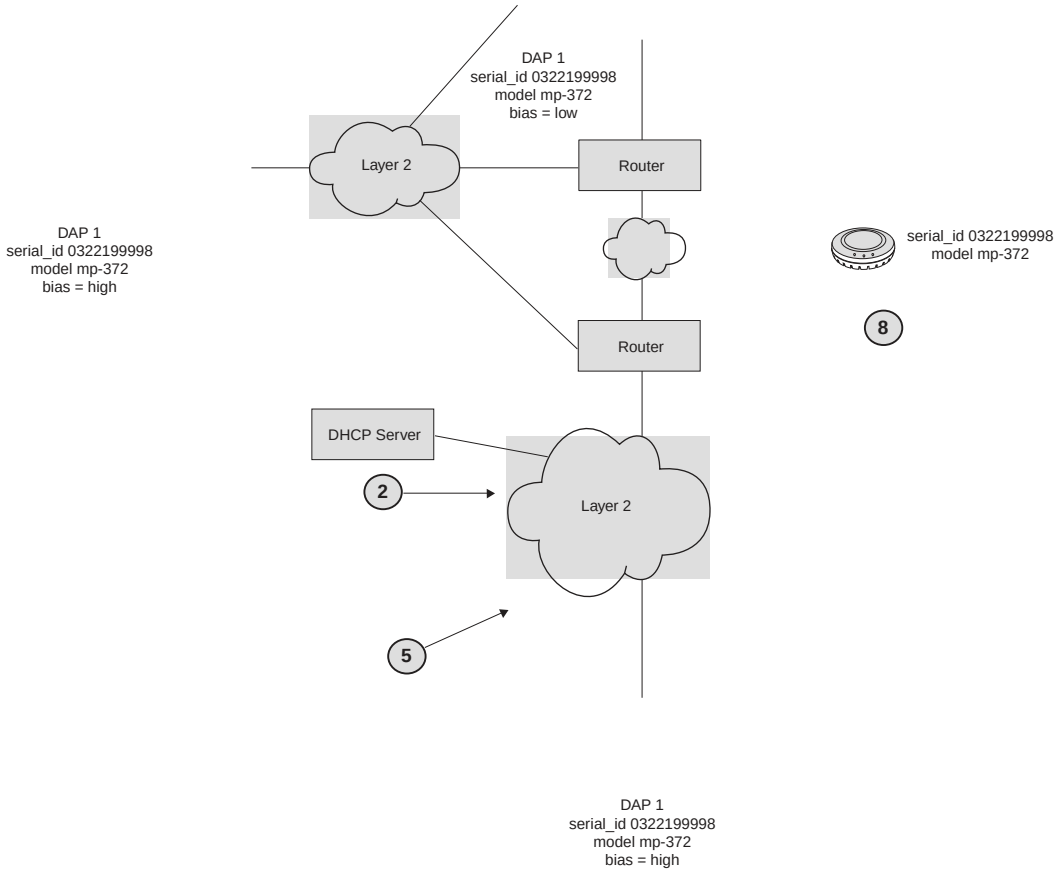

1. The MP sends a DHCP Discover message from the MP port 1.
2. DHCP server receives the Discover message (through a relay agent) and replies with a DHCP Offer message with the IP address for the MP, the router IP address for the MP IP subnet, the DNS server address, and the domain name. MP then sends a DHCP Request message to the server and receives an Ack from the server.
3. The MP sends a broadcast Find MX message to IP subnet broadcast address.
4. MX1 and MX3 have high priority for the MP and reply immediately.
5. The MP contacts MX1 and determines if it should use a locally stored operational image or download it from the MX.

   MX1 is contacted because it has fewer active MP connections than MX3. Once the operational image is loaded, the MP requests configuration information from MX1.

## Example of an MP Booting over a Layer 3 Network

**Figure 12–3** shows an example of the boot process for an MP connected through a Layer 3 network.

**Figure 12–3. An MP Booting over a Layer 3 Network**




1. The MP sends DHCP Discover message from port 1 on the MP.
2. The DHCP server replies with a DHCP Offer message containing an IP address for the MP, the default router IP address for the MP IP subnet, the DNS server address, and the domain name. MP then sends a DHCP Request message to the server and receives an Ack from the server.
3. The MP sends a broadcast Find MX message to the IP subnet broadcast address.
4. When the MP is unable to locate an MX on the subnet connected to it, the MP then sends a DNS request for and .
5. The DNS server sends the system IP address of the MX mapped to or . In this example, the address is for MX1.
6. The MP sends a unicast Find MX message to MX1.
7. MX1 receives the Find MX message and compares the bias settings on each MX for the MP. More than one MX has a high bias for the MP, so MX1 selects the MX with the greatest capacity to add new active MP connections. In this example, MX1 has more capacity. MX1 sends its IP address in the Find MX Reply message to the MP.
8. The MP contacts MX1 and determines to use a locally stored operational image or download it from the MX. Once the operational image is loaded, the MP requests configuration information from MX1.

1. MP sends a DHCP Discover message from the port 1 of the MP.
2. Because MX1 is configured for direct attachment, MX1 responds to the MP and provides the MP with an operational image (or indicates that the MP should use a locally stored image) and configuration from MX1. Only in the event of a physical port failure would the MP attempt to boot from port 2, in which case both MX1 and MX2 would respond to the broadcast Find MX message.

### Example of an MP with a Static IP Configuration Booting on the NetworkMP

**Figure 12–5** shows an example of the boot process for an MP configured with static IP information. In the example, the MP has been configured to use the following:

- Static IP address: 172.16.0.42, netmask: 255.255.255.0, default router 172.16.0.20
- Boot MX : mxr2, DNS server: 172.16.0.1

**Figure 12–5. MP Booting with a Static IP Address**

After the MP is configured with the above information, the next time the MP boots, the following takes place:

1. The MP sends an ARP request for the IP address to discover if the IP address is available.

If the MX is configured with MSS Version 5.0 or later, and the MX has an older image than the MP local image, the MP loads the local image. If the MX is configured with an older MSS version, or the MX has a different image than the MP local image, the MP downloads the operational image from the MX.

The bootloader also compares the MP local image version to the image version on the MX. If the versions do not match, then the image is downloaded from the MX to the MP.

After the operational image is downloaded from the MX, the image is copied into the MP flash memory. The MP reboots, and copies the new version from the flash memory to the RAM. In addition, the MP receives configuration information from the MX and becomes functional on the network as a wireless access point.

## Resiliency and Dual-Homing Options for MPs

MPs can support a wide variety of resiliency options such as redundancy for PoE, for data link connections, and MX services.

- PoE redundancy—On MP models that have two Ethernet ports, you can provide PoE redundancy by connecting both ports to PoE sources. PoE can come from a directly connected

### Dual-Homed Direct Connections to Two MX Switches

**Figure 12–7** shows an example of a dual-homed direct

- The authentication type for users without 802.1X or MAC authentication.


Configuring an SSID name with one character may prevent the SSID from appearing as an available network with the Windows Wireless Client. It is considered a best practice to use more than one character for an SSID name.

**Table 12– 2** lists the parameters controlled by a service profile and the default values.

**Table 12– 2. Defaults for Service Profile Parameters**

| Parameter | Default Value | Radio Behavior When Parameter Set To Default Value |
|---|---|---|
| **11n** | | |

**Table 12– 2. Defaults for Service Profile Parameters (continued)**

| Parameter | Default Value | Radio Behavior When Parameter Set To Default Value |
|---|---|---|
| **max-bw** | **0** | Supports bandwidth control per service profile. Default is unlimited bandwidth per service profile. |
| **mesh** | Not configured | Disables mesh mode by default. |
| **no-broadcast** | **disable** | Does not reduce wireless broadcast traffic by sending unicasts to clients for ARP requests and DHCP Offers and Acks instead of forwarding them as multicasts. |
| **proxy-arp** | **disable** | Does not reply on behalf of wireless clients to ARP requests for client IP addresses. Instead, the radio forwards the ARP Requests as wireless broadcasts. |
| **psk-phrase** | No passphrase defined | Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients. |
| **psk-raw** | No preshared key defined | Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients. |
| **rsn-ie** | **disable** | Does not use the RSN IE in transmitted frames. |
| **shared-key-auth** | **disable** | Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the **set radio-profile auth-psk** command. |
| **short-retry-count** | **5** | Sends a short unicast frame up to five times without acknowledgment. |
| **soda** | **disable** | Sygate On Demand Agent (SODA) files are not downloaded to connecting clients. |
| **ssid-name** | **trapeze** | Uses the SSID name . |
| **ssid-type** | **crypto** | Encrypts wireless traffic for the SSID. |
| **static-cos** | **disable** | Assigns CoS based on the QoS mode (**wmm** or **svp**) or based on ACLs. |
| **tkip-mc-time** | **60000** | Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds. |
| **transmit-rates** | 802.11a:<br>❑ mandatory: **,12.0,24.0**<br>❑ beacon-rate: **6.0**<br>❑ multicast-rate: **auto**<br>❑ disabled: none<br>802.11b:<br>❑ mandatory: **1.0,2.0**<br>❑ beacon-rate: **2.0**<br>❑ multicast-rate: **auto**<br>❑ disabled: none<br>802.11g:<br>❑ mandatory: **1.0,2.0,5.5,11.0**<br>❑ beacon-rate: **2.0**<br>❑ multicast-rate: **auto**<br>❑ disabled: none | Accepts associations only from clients that support one of the mandatory rates.<br>Sends beacons at the specified rate (6 Mbps for 802.11a, 2 Mbps for 802.11b/g).<br>Sends multicast data at the highest rate that can reach all clients connected to the radio.<br>Accepts frames from clients at all valid data rates. (No rates are disabled by default.) |
| **user-idle-timeout** | **180** | Allows a client to remain idle for 180 seconds (3 minutes) before MSS changes the client session to the Disassociated state. |

(To configure a service profile, see **“Configuring a Service Profile” on page 12–30**.)

## Public and Private SSIDs

Each radio can support the following types of SSIDs:

- **Encrypted SSID**—Clients using this SSID must use en

## Radio Profiles

You can easily assign radio configuration parameters to many radios by configuring a radio profile and assigning the profile to the radios. You can enable the radio when you assign the profile.

**Table 12– 3** summarizes the parameters controlled by radio profiles. Generally, the only radio parameters controlled by the profile to modify are the SSIDs

### Default Radio Profile

MSS contains one default radio profile, named default. To apply common parameters to radios, you can modify the default profile or create a new one. When you create a new profile, the radio parameters in the profile are set to the factory default values.

### Radio-Specific Parameters

The channel number, transmit power, and external antenna parameters are unique to each radio and are not controlled by radio profiles. **Table 12– 4** lists the defaults for these parameters.

**Table 12– 4. Radio-Specific Parameters**

| Parameter | Default Value | Description |
|---|---|---|
| **antenna-location** | indoors | Radio antenna location<br><br>**Note:** This parameter applies only to MPs that support external antennas. |
| **antennatype** | For most MP models, the default is **internal**.<br>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**.<br>The default for the 802.11b/g radio on model MP-262 is **ANT1060**. | Trapeze external antenna model<br><br>**Note:** This parameter is configurable only on MPs that support external antennas. |
| **auto-tune max-power** | Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower. | Maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio |
| **channel** | ❑ 802.11b/g—**6**<br>❑ 802.11a—Lowest valid channel number for the country of operation | Channel number that a radio transmits and receives traffic. |
| **mode** | **disable** | Operational state of the radio. |
| **radio-profile** | None. You must add the radios to a radio profile. | 802.11 settings |
| **tx-power** | Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower. | Transmit power of a radio, in decibels referred to 1 milliwatt (dBm) |

Although these parameters have default values, Trapeze Networks recommends that you change the values for each radio for optimal performance. For example, leaving the channel number on each radio set to the default value can result in high interference among the radios.

## Configuring MPs

To configure MPs, perform the following tasks:

- Specify the country of operation. (See **"Specifying the Country of Operation" on page 12–18**.)
- Configure an Auto-AP profile for automatic configuration of Distributed MPs. (See **"Configuring an Auto-AP Profile for Automatic MP Configuration" on page 12–21**.)
- Configure MP access ports and dual homing. (See **"Configuring MP Port Parameters" on page 12–25**.)
- Configure MP-MX security. (See **"Configuring MP-MX Security" on page 12–28**.)
- Configure a service profile to set SSID and encryption parameters. (See **"Configuring a Service Profile" on page 12–30**.)
- Configure a radio profile. (See **"Configuring a Radio Profile" on page 12–34**.)

- If required, configure the channel, transmit power, and external antenna type on each radio. (See **"Configuring Radio-Specific Parameters" on page 12–38**.)
- Map the radio profile to a service profile. (See **"Mapping the Radio Profile to Service Profiles" on page 12–39**.)
- Assign the radio profile to radios and enable the radios. (See **"Assigning a Radio Profile and Enabling Radios" on page 12–39**.)

## Specifying the Country of Operation

You must specify the country in which you plan to operate the MX and the MPs. MSS does not allow you to configure or enable the MP radios until you specify the country of operation.


To specify the country, use the following command:

`set system countrycode` *code*

For the country, you can specify one of the codes listed in **Table 12– 5**.

**Table 12– 5. Country Codes (continued)**

| Country | Code |
|---|---|
| El Salvador | **SV** |
| Egypt | **EG** |
| Estonia | **EE** |
| Finland | **FI** |
| France | **FR** |
| Germany | **DE** |
| Greece | **GR** |
| Grenada | GD |
| Guatemala | **GT** |
| Honduras | **HN** |
| Hong Kong | **HK** |
| Hungary | **HU** |
| Iceland | **IS** |
| India | **IN** |
| Indonesia | **ID** |
| Ireland | **IE** |
| Israel | **IL** |
| Italy | **IT** |
| Jamaica | **JM** |
| Japan | **JP** |
| Jordan | **JO** |
| Kazakhstan | **KZ** |
| Kenya | **KE** |
| St. Kitts and Nevis | **KN** |
| Kuwait | **KW** |
| Cayman Islands | KY |
| Latvia | **LV** |
| Lebanon | **LB** |
| Liechtenstein | **LI** |
| Lithuania | **LT** |
| St. Lucia | **LC** |
| Luxembourg | **LU** |
| Malaysia | **MY** |
| Malta | **MT** |
| Mauritius | **MU** |
| Mexico | **MX** |
| Monserrat | MS |
| Morocco | **MA** |
| Namibia | **NA** |
| Netherlands | **NL** |
| New Zealand | **NZ** |

**Table 12– 5. Country Codes (continued)**

| Country | Code |
|---|---|
| Nigeria | **NG** |
| Norway | **NO** |
| Oman | **OM** |
| Pakistan | **PK** |
| Panama | **PA** |
| Paraguay | **PY** |
| Peru | **PE** |
| Philippines | **PH** |
| Poland | **PL** |
| Portugal | **PT** |
| Puerto Rico | **PR** |
| 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** |
| Trinidad and Tobago | **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** |
| Zambia | **ZM** |
| Zimbabwe | **ZW** |

To verify the configuration change, use the following command:

```
show system
```

The following commands set the country code to US (United States) and verify the setting:

```
MX# set system countrycode  S
success: change accepted.
MX# show system
================================================================================
 Product Name:       MX
 System Name:        MX
 System Countrycode:  S
 System Location:
 System Contact:
 System IP:          30.30.30.2
 System idle timeout:3600
 System MAC:         00:0B:0E:02:76:F6
================================================================================
 Boot  ime:          2003-05-07 08:28:39
  ptime:                 0 days 04:00:07
================================================================================
 Fan status:             fan1 OK fan2 OK fan3 OK
  emperature:            temp1 ok  temp2 ok  temp3 ok
 PS  Status:             Lower Power Supply DC ok AC ok   pper Power Supply missing
 Memory:                 115.09/496.04 (23%)
  otal POE Draw [W]    : 32.000
================================================================================
```

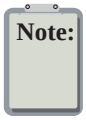
## Configuring an Auto-AP Profile for Automatic MP Configuration

You can use an Auto-AP profile to deploy unconfigured Distributed MPs. A Distributed MP that does not have a configuration on an MX can receive a configuration file from the Auto-AP profile instead.

From the range of available valid MP numbers on the MX, the Auto-AP profile assigns a Distributed MP number and name to the MP. The Auto-AP profile also configures the MP and radio parameter settings in the profile. (See “Configuring an Auto-AP Profile” on page 22.)

The Auto-AP profile does not configure SSIDs, encryption parameters, or any other parameters managed by service profiles. You still need to configure a service profile separately for each SSID.

An MX can have one Auto-AP profile.




### Locating an MX for Automatic MP Configuration

The boot process for unconfigured Distributed MP on an MX is similar to the process for configured Distributed MPs. After the MP starts up, the MP uses DHCP to configure the IP connection to the network. The MP then uses the IP connection to contact an MX switch.

The MX contacted by the MP determines the best MX for configuring the MP, and sends the MX IP address to the MP. The best switch to use for configuring the MP is one that has an Auto-AP profile with a high bias setting. If more than one MX has an Auto-AP profile with a high bias setting, the MX with the greatest capacity to add new unconfigured MPs is selected.

An MX with the capacity to add a new unconfigured Distributed MP meets the minimum of the following criteria:

- Maximum number of MPs configurable on the MX, minus the number already configured.
- Maximum number of MPs active on the MX, minus the number already active.

For example, suppose the Mobility Domain has two MX switches, with the capacities and loads listed in **Table 12– 6**.

For MX-8A:

- The Number of MPs that can be configured on the MX, minus the number currently configured, is 30 - 25 = 5.
- The Number of MPs that can be active on the MX, minus the number currently active, is 12 - 8 = 4.
- The lesser of the two values is 4. The MX can add up to 4 more MPs.

For MX-8B:

- The Number of MPs that can be configured on the MX, minus the number currently configured, is 30 - 20 = 10.
- The Number of MPs that can be active on the MX, minus the number currently active, is 12 - 12 = 0.
- The lesser of the two values is 0. The MX cannot add more MPs.

MX-8A has the capacity to add 4 more MPs, whereas MX-8B cannot add any more MPs. Therefore, the contacted MX sends the IP address of MX-8A to the MP. The MP then requests a software image file and configuration from MX-8A.

## Configured MPs Have Precedence Over Unconfigured MPs

When an MX determines the MX IP address to send to a booting MP, the MX gives preference to MPs previously configured instead of unconfigured MPs that require an Auto-AP profile. The MX can direct a configured MP to a MX with active MPs configured using the Auto-AP profile, even if the MX does not have capacity for more active MPs. In this case, the MX randomly selects an MP with an Auto-AP profile to disconnect, and acce

```
tx pwr: 15, profile: default
auto-tune max-power: default
Radio 2: type: 802.11a, mode:  enabled, channel: dynamic
tx pwr: 11, profile: default
auto-tune max-power: default
```

This example shows the defaults for the MP parameters you can configure in the Auto-AP profile. **Table 12– 7** lists the configurable Auto-AP profile parameters and their defaults. The only parameter that requires configuration is the Auto-AP profile mode. The Auto-AP profile is disabled by default. To use the Auto-AP profile to configure Distributed MPs, you must enable the profile. (See "Enabling the Auto-AP Profile" on page 24.)

**Table 12– 7. Configurable Profile Parameters for Distributed MPs**

| Parameter | | Default Value |
|---|---|---|
| **MP Parameters** | | |
| **bias** | | **high** |
| **blink** | | **disable** |
| **contact** | | **none** |
| **force-image-download** | | **disable (NO)** |
| **group** (load balancing group) | | none |
| **mode** | | **disabled** |
| **persistent** | | none |
| **timeout** | | 10 seconds |
| **upgrade-firmware** (boot-download-enable) | | **enable (YES)** |
| **Radio Parameters** | | |
| **radio** | **auto-tune max-power** | **default** |
| **radio** | **mode** | **enabled** |
| **radio** | **radio-profile** | **default** |
| **radiotype** | | **11g** (or **11b** for country codes where 802.11g is not allowed) |

Also, the SSIDs and encryption settings are configured from the service profiles mapped to the radio profile. To use a radio profile other than , you must specify the radio profile. (See "Specifying the Radio Profile Used by the Auto-AP Profile" on page 24.)

## Changing MP Parameter Values

The commands for configuring MP and radio parameters for the Auto-AP profile are identical to the commands for configuring an individual Distributed MP. Instead of specifying a Distributed MP number with the command, specify **auto**. For more information about the syntax, see the "MP Commands" chapter of the .

```
MP Parameters:
set ap auto bias {high | low}
set ap auto blink {enable | disable}
set ap auto force-image-download {enable | disable}
set ap auto group name
set ap auto mode {enable | disable}
set ap auto persistent [apnum | all]
set ap auto upgrade-firmware {enable | disable}
Radio Parameters:
set ap auto radiotype {11a | 11b| 11g}
set ap auto radio {1 | 2} auto-tune max-power power-level
set ap auto radio {1 | 2} mode {enable | disable}
set ap auto radio {1 | 2} radio-profile name mode {enable | disable}
```

### Enabling the Auto-AP Profile

To enable the Auto-AP profile for automatic Distributed MP configuration, type the following command:

```
MX# set ap auto mode enable
success: change accepted.
```

### Specifying the Radio Profile Used by the Auto-AP Profile

The Auto-AP profile uses radio profile by default. To use another radio profile instead, use

The MP continues to operate without interruption after you enter the **set ap auto persistent** command. The next time the MP is restarted, the Auto-AP profile is not used to configure the MP. Instead, the persistent configuration is used. (Use the

## Configuring Static IP Addresses on Distributed MPs

By default, Distributed MPs use the procedure described in **"Distributed MPs and DHCP Option 43" on page 12–4** to obtain an IP address and connect to an MX. In some installations, DHCP may not be available. In such a case, you can manually assign static IP address information to the MP.

You can also optionally specify the MX that the Distributed MP uses as the boot device, and an 802.1Q VLAN tag to be applied to Ethernet frames sent from the distributed MP.

When you configure static IP information for a Distributed MP, the MP uses the boot procedure described in **"MP Booting with a Static IP Address" on page 12–8** instead of the default boot procedure.

```
MX# set ap 1 boot-configuration vlan vlan-tag 100 mode enable
success: change accepted.
```

## Clearing an MP from the Configuration

To clear the port settings from a port, use the following command:

```
clear port type port-list
```

This command resets the port as a network port and removes all MP-related parameters from the port.

To clear an MP, use the following command:

```
clear ap apnum
```

## Changing MP Names

The default name of a directly attached MP is based on the port number of the MP access port. For example, the default name for an MP on MP access port 1 is . The default name of a Distributed MP is based on the number you assign to it when you configure the connection. For example, the default name for Distributed MP 1 is .

MP names appear in the output of some CLI **show** commands and in RingMaster. To change the name of an MP, use the following command:

```
set ap apnum name name
```

## Changing Bias

The CLI commands described in this section enable you to change the bias for an MP.

To change the bias of an MP, use the following command:

```
set ap apnum bias {high | sticky | low}
```

The default bias is high.

To change the bias for a Distributed MP to low, type the following command:

```
MX# set ap 1 bias low
success: change accepted.
```

## Disabling or Reenabling Automatic Firmware Upgrades

An MP can automatically upgrade the boot firmware by loading a later version of the firmware from an MX when the MP is booting. Automatic firmware upgrades are enabled by default.

To disable or reenable automatic firmware upgrades, use the following command:

```
set ap apnum upgrade-firmware {enable | disable}
```

## Enabling LED Blink Mode

Blink mode makes an MP easy to identify. When blink mode is enabled on MPs, 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, LED blink mode is disabled. If enabled, blink mode continues until you disable it.

Changing the LED blink mode does not alter operation of the MP. Only the behavior of the LEDs is affected.

To enable or disable LED blink mode, use the following command:

```
set ap apnum blink {enable | disable}
```

### Configuring AP Communication Time Out

You can configure the communication time out on a MP using the following command”

```
set ap apnum time-out seconds
```

The length of time can be set from 1 to 180 seconds. The default value is 10 seconds.

## Configuring MP-MX Security

MSS provides security for management traffic between MX switches and Distributed MPs. When the feature is enabled, all management traffic between Distributed MPs that support encryption and the MX is encrypted. MP-MX security is set to **optional** by default.

The encryption uses RSeelic key rypti]TJ22.7415 0 TD.0012 Tc-.0048 Tw[(tosste5.47e)-3.19(m, itch AES-CCM)]T.

**Table 12– 9** lists the MP security options and whether an MP can establish a management session with an MX based on the option settings.

## Verifying an MP Fingerprint on an MX

To verify an MP fingerprint, find the fingerprint and use the **set ap fingerprint** command to enter the fingerprint in MSS.

### Finding the Fingerprint

The MP fingerprint is listed on a label on the back of the MP. (See “Encryption Key Fingerprint” on page 28.)

If the MP is already installed and operating, use the **show ap status** command to display the fingerprint. The following example shows information for MP 8, including the fingerprint:

```
MX# show ap status 8
AP: 7, AP model: MP-252, manufacturer  rapeze, name: MP07
         fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
==================================================
State:     operational (not encrypted)
CP  info:  IBM:PPC speed=266666664 Hz version=405GPr
                  id=0x29f1886d447f111a ram=33554432
                  s/n=0424000779 hw_rev=A3
 ptime:    1 hours, 8 minutes, 17 seconds
```

`set ap` *`apnum`* `fingerprint` *`hex`*

where is the 16-digit hexadecimal number of the fingerprint. Use a colon

You can configure different data rates on the MP-432 for 802.11b, 802.11ng, and 802.11na.

| | |
|---|---|
| 802.11na | 6.0, 9.0,12.0, 18.0, 24.0, 36.0, 48.0, 54.0, MCS0-15 |
| 802.11b | 1.0, 2.0, 5.5, 11.0 |
| 802.11ng | 1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0, MCS0-15 |

## PoE Requirements

PoE support is different for the MP-432 because the MP has two 802.11n radios and requires more PoE support than a single 802.3af power source. There are two possible configurations for supplying power to the MP-432:

- If the power mode is set to “auto”, the power is managed automatically by sensing the power level on the AP. If low power is detected, unused Ethernet is disabled and reduces the traffic on the 2.4 GHz radio. If high power is detected, then both radios operate at 3x3 (3 transmit chains and 3 receive chains).
- If the power mode is set to “high”, both radios operate at the maximum power available which requires either 802.3at PoE or both ports using 802.3af PoE.
- **set ap <*apnum*> power-mode <auto | high>**

## Glossary of Terms for 802.11n

| | |
|---|---|
| A-MPDU<br>(Aggregate MAC Protocol Data Unit) | Allows multiple MPDUs to be transmitted as a single PDU frame. This is configured as 8K, 16K, 32K, or 64K. |
| A-MSDU<br>(Aggregate MAC Service Data Unit) | Allows multiple MSDUs to be tr |

### Configuration Commands

```
MXR2# ꞓe  a  apnum  ꞏ  portnum  ꞓe {2330 | 2330A | AP2750 | AP3750 | AP3850 |
        MP-352 | MP-371 | MP-372 | MP-372-JP | MP-372A | MP-372-CN | MP-372-JP |
        MP-422 | MP-422A | MP-422F| MP-432 | MP-620 | MP-620A | MP-71}  e {enable |
        disable} radiotype {11a| 11b|11g | 11na|11ng}
```

### Frame Aggregation Commands

```
MXR2# ꞓe  ꞓeꞏ  e- ꞏ  e profile-name 11  a- ꞓ- a/ - e  [8K| 16K| 32K| 64K]
      a- ꞓ- a/ - e  [4K | 8K]  ꞏa e-a  ꞏe a  [msdu|mpdu|all|disable]
      {  ꞓe- a  ꞓe-  [enable|disable| required]}
      ꞓ  ꞏ  - a ꞏ  eꞏ a  [enable disable]
```

### Data Rate Commands

```
MXR2# ٤e  ٤eH   e- H    e profile-name  Ha ٤   -Ha e٤ 11    a a  H
        {1.0|2.0|5.5|6.0|9.0|11.0|12.0|18.0|24.0|36.0|48.0|54.0|m0|m1|m2|m3|m4|m5|
        m6|m7|m8|m9|m10|m11|m12|m13|m14|m15} bea   -Ha e <radio-rate>
        a ٤ab e a U    a٤ -Ha e {auto|1.0|2.0|5.5|6.018.0|24.0|36.0|48.0|54.0|
        m0|m1|m2|m3|m4|m5|m6|m7|m8|m9|m10|m11|m12|m13|m14|m15}

MXR2# ٤e  ٤eH   e- H    e profile-name  Ha ٤   -Ha e٤ 11 a  a a  H
        {6.0|9.0|12.0|18.0|24.0|36.0|48.0|54.0|m0|m1|m2|m3|m4|m5|m6|m7|m8|m9|m10|
        m11|m12|m13|m14|m15} bea   -Ha e <radio-rate> a ٤ab e a U    a٤ -Ha e
        {auto|6.0|9.0|12.0|18.0|24.0|36.0|48.0|54.0|m0|m1|m2|m3|m4|m5|m6|m7|m8|m9|
        m10|m11|m12|m13|m14|m15}
```

### 11n Channel Commands

```
MXR2# ٤e  Haa - H    e profile-name 11    a  e -  a - a {20MHz | 40MHz}


MX#
```

# Displaying MP Information

You can display the following MP information:

- MP and radio-specific configuration settings
- Connection information for Distributed MPs configured on an MX
- List of Distributed MPs not configured on an MX
- Connection information for Distributed MPs
- Service profile information
- Radio profile information
- Status information
- Information about static IP addresses on Distributed MPs
- Statistics counters
- Information about VLAN profiles configured for local switching
- ARP table on an MP
- Forwarding Database (FDB) for an MP
- Information about the VLANs locally switched by an MP
- Information about ACLs used by the MP

## Displaying MP Configuration Information

To display configuration information, use the following commands:

`show ap config [apnum [radio {1 | 2}]]`

The command lists information separately for each MP.

To display configuration information for MP 59, type the following command:

```
MX# show ap config 4
AP 4 (AP04)
Model: MP-422
Mode:
Bias: high
Power mode: auto
Options: upgrade-firmware
Connection: netbc7E33.4netbc7E33.y0 -1oer: 0675200557
Fingerprint:
Communication timeout: 2533.4netbc7Location:
```

```
Contact:
Vlan-profile: default

Radio 1 (802.11g)
Mode: sentry          Radio profile: default
Channel: dynamic      Load balancing: YES
Tx power: 22          Load balancing group:
Autotune max power: default       Force rebalance: NO
Antenna location: indoors         Antenna type: INTERNAL
Service profiles:
Snoop filters on radio: none
Snoop filters on radio profile: none

Radio 2 (802.11a)
Mode: enabled Radio profile: mirunaMeshOne
Channel: 36 Load balancing: YES
Tx power: 5 Load balancing group:
Auto tune max power: default Force rebalance: NO
Antenna location: indoors Antenna type: INTERNAL
Service profiles:
mirunaMeshOne (Mesh)
Snoop filters on radio: none
Snoop filters on radio profile: none
```

(For information about the fields in the output, see the .)

## Displaying Connection Information for Distributed MPs

To display connection information for Distributed MPs configured on an MX, use the following command:

`show ap global [`*`apnum`* `|` `serial-id` *`serial-ID`*`]`

This command lists the System IP addresses of all the MX switches configured with each Distributed MP, and lists the bias for the MP on each MX. For each Distributed MP that is configured on the local MX, the connection number is also listed.

Connections are shown only for the Distributed MPs that are configured on the MX where the command is entered, and only for the Mobility Domain the MX is in.

To display connection information for all MPs configured on an MX, type the following command:

```
MX# show ap global
 otal 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
```

This command indicates that four Distributed MPs are configured on the MX, with serial IDs , , , and . Each MP is also configured on one of two other MX switches, with system IP addresses 10.3.8.111 and 10.4.3.2. The bias for the MP on each MX is listed. Normally, a Distributed MP boots from the MX with the high bias for the MP. (For more information, see **“” on page 12–9** and **“Boot Process for Distributed MPs” on page 12–4**.)

The AP field indicates the connection number of each MP on the MX on which the command is typed. A hyphen ( - ) in the AP field indicates that the MP is config

obility Domai. 3

To change transmit rates for a service profile, use the following command:

## Disabling Idle-Client Probing

By default, an MP radio sends keepalive messages (idle-client probes) every 10 seconds to each client with an active session on the radio, to verify that the client is still active. The probes are unicast null-data frames. Normally, an active client sends an Ack in reply to an idle-client probe.

If a client does not send any data or respond to any idle-client probes before the user idle timeout expires (see **"Changing the User Idle Timeout" on page 13–4**), MSS changes the client session to the Disassociated state.

Responding to keepalive messages requires power use by a client. If you need to conserve power on the client (for example, on a VoIP handset), you can disable idle-client probing.

To disable or reenable idle-client probing, use the following command:

```
set service-profile profile-name idle-client-probing {enable | disable}
```

The following command disables idle-client probing on service profile :

```
MX# set service-profile sp1 idle-client-probing disable
success: change accepted.
```

## Changing the User Idle Timeout

The user idle timeout specifies the number of seconds a client can remain idle before the MX changes the client session to the Disassociated state. A client is considered to be idle if it does not send data and does not respond to idle-client probes. You can specify a timeout value from 20 to 86400 seconds. The default is 180 seconds (3 minutes). To disable the user-idle timeout, set the value to 0.

To change the user-idle timeout, use the following command:

```
set service-profile profile-name user-idle-timeout seconds
```

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.
```

## Changing the Short Retry Threshold

The short retry threshold specifies the number of times a radio can send a short unicast frame for an SSID without receiving an acknowledgment for the frame. A short unicast frame is a frame that is than the RTS threshold.

To change the short retry threshold, use the following command:

```
set service-profile profile-name short-retry threshold
```

The threshold can be a value from 1 through 15. The default is 5.

To change the short retry threshold for service profile to 3, type the following command:

```
MX# set service-profile sp1 short-retry 3
success: change accepted.
```

## Changing the Long Retry Threshold

The long retry threshold specifies the number of times a radio can send a long unicast frame for an SSID without receiving an acknowledgment for the frame. A long unicast frame is a frame that is the RTS threshold.

To change the long retry threshold, use the following command:

```
set service-profile profile-name long-retry threshold
```

The threshold can be a value from 1 through 15. The default is 5.

To change the long retry threshold for service profile to 8, type the following command:

```
MX# set service-profile sp1 long-retry 8
success: change accepted.
```

# Configuring a Radio Profile

A radio profile is a set of parameters that apply to multiple radios. You can easily assign configuration parameters to many radios by configuring a profile and assigning the profile to the radios.

To configure a radio profile:

- Create a new profile.
- Change radio parameters.
- Map the radio profile to one or more service profiles.

(For a list of the parameters controlled by radio profiles and their defaults, see Table 9– 3 on page 16.)

The channel number, transmit power, and external antenna type are unique to each radio and are not controlled by radio profiles. (To configure these parameters, see **"Configuring Radio-Specific Parameters" on page 13–8**.)

(To display radio profile information, see **"Displaying Radio Profile Information" on page 13–14**.)

## Creating a New Profile

To create a radio profile, use the following command:

```
set radio-profile profile-name [mode {enable | disable}]
```

### Changing the DTIM Interval

The DTIM interval specifies the number of times after every beacon that a radio sends a delivery traffic indication map (DTIM). An MP access point sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM. The DTIM interval applies to both the beaconed SSID and the unbeaconed SSID.

The DTIM interval does not apply to unicast frames. An MP also stores unicast frames in buffer memory, but the MP includes information about the buffered unicast frames in each beacon frame. When a user station receives a beacon frame that advertises unicast frames destined for the station, the station sends a request for the frames and the MP transmits the requested frames to the user station.

To change the DTIM interval, use the following command:

```
set radio-profile profile-name dtim-interval interval
```

The interval can be a value from 1 through 31. The default is 1.

To change the DTIM interval for radio profile to 2, type the following command:

```
MX# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

### Changing the RTS Threshold

e

The time can be from 500 ms (0.5 second) through 250,000 ms (250 seconds). The default is 2000 ms (2 seconds).

To change the maximum receive threshold for radio profile to 4000 ms, type the following command:

```
MX# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

### Changing the Maximum Transmit Threshold

The maximum transmission threshold specifies the number of milliseconds a frame by a radio can remain in buffer memory. To change the maximum transmit lifetime, use the following command:

```
set radio-profile profile-name max-tx-lifetime time
```

The time can be from 500 ms (0.5 second) through 250,000 ms (250 seconds). The default is 2000 ms (2 seconds).

To change the maximum transmit threshold for radio profile to 4000 ms, type the following command:

```
MX# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

### Changing the Preamble Length

By default, 802.11b/g radios advertise support for frames with short preambles and can support frames with short or long preambles.

An 802.11b/g radio generates unicast frames to send to a client with the specified preamble length. An 802.11b/g radio always uses a long preamble in beacons, probe responses, and other broadcast or multicast traffic.

Generally, clients assume access points require long preambles and request to use short preambles only if the associated access point advertises support for short preambles. You can disable the advertisement of support for short preambles by setting the preamble length value to **long**. In this case, clients assume that the access point supports long preambles only and the clients request long preambles.

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.

If any client associated with an 802.11b/g radio uses long preambles for unicast traffic, the MP still accepts frames with short preambles but does not transmit any frames with short preambles. This change also occurs if the MP overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

The default preamble length value is **short**. This command does not apply to 802.11a radios.

To change the preamble length advertised by 802.11b/g radios, use the following command:

```
set radio-profile profile-name preamble-length {long | short}
```

To configure 802.11b/g radios that use the radio profile advertise support for long preambles instead of short preambles, type the following command:

```
MX# set radio-profile rp_long preamble-length long
success: change accepted.
```

## Resetting a Radio Profile Parameter to the Default Value

To reset a radio profile parameter to default values, use the following command:

```
clear radio-profile profile-name parameter
```

The can be one of the radio profile parameters listed in Table 9– 3 on page 16.


Make sure you specify the radio profile parameter you want to reset. If you do not specify a parameter, MSS deletes the entire profile from the configuration.

All radios that use this profile must be disabled before you can delete the profile. If you specify a parameter, the setting for the parameter is reset to the default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration.

To disable the radios that are using radio profile and reset the **beaconed-ssid** parameter to its default value, type the following commands:

```
MX# set radio-profile rp1 mode disable
MX# clear radio-profile rp1 beaconed-ssid
success: change accepted.
```

### Removing a Radio Profile

To remove a radio profile, use the following command:

```
clear radio-profile name
```


You must disable all radios that are using a radio profile before you can remove the profile. (See **"Disabling or Enabling All Radios Using a Profile" on page 13–11**.)

To disable the radios that are using radio profile and remove the profile, type the following commands:

```
MX# set radio-profile rptest mode disable
MX# clear radio-profile rptest
success: change accepted.
```

## Configuring Radio-Specific Parameters

This section shows how to configure the channel and transmit power on individual radios, and how to configure for external antennas. (For information about the parameters you can set on individual radios, see **Table 9– 4**.)

### Configuring the Channel and Transmit Power


If RF Auto-Tuning is enabled for channels or power, you cannot set the channels or power manually using the commands in this section.

To set the channel and transmit power of a radio, use the following commands:

```
set ap apnum radio {1 | 2} channel channel-number
set ap apnum radio {1 | 2} tx-power power-level
```

The parameters are shown in separate commands for simplicity. However, you can use the **channel** and **tx-power** parameters on the same command line.

Specify **1** or **2** for the radio number:

- For a single-radio model, specify

To specify the external antenna model, use the following command:

```
set ap apnum radio {1 | 2} antennatype {AN 1060 | AN 1120 | AN 1180 |
         AN 5060 | AN 5120 | AN 5180 | AN 7360
         AN -1360-O   | AN -5360-O   | AN -5060-O   | AN -5120-O   |
         AN -7360-O   | internal}
```

To configure antenna model ANT-1060 for an MP-372 on MP 1, type the following command:

```
MX# set ap 1 radio 1 antennatype AN 1060
success: change accepted.
```

```
set ap apnum radio {1 | 2} mode {enable | disable}
```

To disable radio 2 on port 3 and 7, type the following command:

```
MX# set ap 3,7 radio 2 mode disable
success: change accepted.
```

## Disabling or Enabling All Radios Using a Profile

To disable or enable all radios that are using a radio profile, use the following command:

```
set radio-profile profile-name [mode {enable | disable}]
```

The following command enables all radios that use radio profile :

```
MX# set radio-profile rp1 mode enable
success: change accepted.
```

The following commands disable all radios that use radio profile , change the beacon interval, then reenable the radios:

```
MX# set radio-profile rp1 mode disable
success: change accepted.
MX# set radio-profile rp1 beacon-interval 200
success: change accepted.
MX# set radio-profile rp1 mode enable
success: change accepted.
```

## Resetting a Radio to Factory Default Settings

To disable an MP radio and reset it to the factory default settings, use the following command:

```
clear ap apnum radio {1 | 2 | all}
```

This command performs the following actions:

- Sets the transmit power, channel, and external antenna type to the default values.
- Removes the radio from a radio profile and places the radio in the default radio profile.

This command does not affect the PoE setting.

When local switching is enabled, the client VLAN is directly accessible through the wired interface on the MP. Packets can be switched directly to and from this interface.

Normally, when local switching is disabled on an MP, packets are tunneled through the network back to an MX, and traffic is placed on the client VLAN. This process requires packets to be encapsulated, unencapsulated, and possibly fragmented, which may introduce latency in the switching path. Omitting the MX from the forwarding path for client traffic eliminates the tunnel encapsulation process, which can result in improved network performance.

Local packet switching is disabled by default. An MP can be configured to switch packets for some VLANs locally and tunnel packets for other VLANs through the MX switch.

### Notes

- Restricting Layer 2 forwarding for a VLAN is not supported if the VLAN is configured for local switching.
- The DHCP restrict feature is not supported for locally switched clients.
- Web Portal is not supported for locally switched clients.
- W hen the **set ap <*apnum*> port <*portnum*> type** command is used to specify a port on a directly attached MP, the MP cannot be configured to perform local switching. However, a directly connected MP with an unspecified port can perform local switching.
- IGMP snooping is not supported with local switching.

## Configuring Local Switching

Configuring an MP to perform local switching consists of the following tasks:

- Configuring a for the MP that specifies the VLANs to be locally switched.
- Enabling local switching on the MP.
- Applying the VLAN profile to the MP.

In addition, the VLAN profile can be cleared from the MP, or removed from the MX.

### Configuring a VLAN Profile

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 the MX.

inmedi2(rath )ng Layerof.1( )j1J-27/7-94-1.10848D.0021 fc.0028 fwng Layured att.ath

To add VLANs to a VLAN profile, use the following command:

```
set vlan-profile profile-name vlan vlan-name [tag tag-value]
```

Enter a separate.8(wev)4.2(e)3.2trafile--2.9(.5)p(N prtt)6.ofile

```
Auth fallthru:              last-resort   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    ser idle timeout:                180
Idle client probing:                yes   Keep initial vlan:                no
Web Portal Session  imeout:           5   Mesh enabled:                     no
Web Portal ACL:                           Bridging enabled:                 no
Load Balance Exempt:                 no   Web Portal Logout:                no
Custom Web Portal Logout  RL:
vlan-name = default
11a beacon rate:                    6.0   multicast rate:                 A  O
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:                 A  O
11b mandatory rate: 1.0,2.0 standard rates: 5.5,11.0
11g beacon rate:                    2.0   multicast rate:                 A  O
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
```

(For information about the fields in the output, see the .)

## Displaying Radio Profile Information

To display radio profile information, use the following command:

```
show radio-profile {profile-name | ?}
```

Entering **show radio-profile ?** displays a list of radio profiles.

To display radio profile information for the default radio profile, type the following command:

```
MX# show radio-profile default
Beacon Interval:                  100   D IM Interval:                      1
Max  x Lifetime:                 2000   Max Rx Lifetime:                 2000
R S  hreshold:                   2346   Frag  hreshold:                  2346
Long Preamble:                     no    une Channel:                     yes
 une Channel Range (11a):  lower-bands   Ignore Clients:                   no
 une Power:                        no    une Channel Interval:            3600
 une Power Interval:              600   Power ramp interval:               60
Channel Holddown:                 300   Countermeasures:                 none
Active-Scan:                      yes   RFID enabled:                      no
WMM Powersave:                     no   QoS Mode:                         wmm
Rate Enforcement:                  no   Initial Load:                    1000
E   Link Factor:                    3   Change  hreshold:                  25
Dwell  ime:                      3600   Probe Interval:                    60
Initial Measure Interval:          60   Maximum Measure Interval:         600
Radio Link  imeout:                 5
```

(For information about the fields in the output, see the )

```
      LastPktRxSigStrengo(tPs  12 5  go(tP     Mulas)6.7iBytDroas)6.p       asLastPSigNastP
```

```
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
```

(For information about the fields in the output, see the .)

## Displaying the Forwarding Database for an MP

To display the entries in a specified MP forwarding database, use the following command:

```
show ap fdb apnum
```

The following command displays FDB entries for AP 7:

```
MX# show ap fdb 7
AP 7:
# = System Entry. $ = Authenticate Entry
VLAN  AG  Dest MAC/Route Des [CoS] Destination Ports
---- ---- ------------------ ----- -----------------
4095 4095 00:0b:0e:00:ca:c1      #          CP
4095    0 00:0b:0e:00:04:0c                eth0
```

(For information about the fields in the output, see the .)

## Displaying VLAN Information for an MP

To display information about the VLANs that are either locally switched by the specified MP or tunneled from the MP to an MX, use the following command:

```
show ap vlan apnum
```

The command lists the VLANs to which the clients associated with the MP are members, and whether traffic for each VLAN is locally switched or tunneled back to an MX.

The following command displays information about the VLANs switched by AP 7:

```
MX# show ap vlan 7
AP 7:
VLAN Name             Mode    Port               ag
---- ---------------- ----    ---------------- ----
   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
```

(For information about the fields in the output, see the .)

## Displaying ACL Information for an MP

When an MP is configured to perform local switching, you can display the number of packets filtered by security ACLs (“hits”) on the MP. Each time a packet is filtered by a security ACL, the MP ACL hit counter increments. To display ACL hits for an MP, use the following command:

```
show ap acl hits apnum
```

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.

The following command displays the security ACL hits on MP 7,

```
MX# show ap acl hits 7
ACL hit-counters for AP 7
Index Counter              ACL-name
----- -------------------- --------
```

13

# Configuring WLAN Mesh Services

## WLAN Mesh Services Overview

allow an MP to provide wireless services to clients without a wired interface on the MP. Instead of a wired interface, there is a radio link to another MP with a wired interface.There are three components to a mesh deployment:

- Mesh Portal – the MP connected to the wired port on an MX.
- Mesh MP – the wireless MP without a wired connection (untethered)
- Mesh Link – a Layer 2 transparent bridge with the Mesh Portal and the Mesh MP as endpoints.

WLAN mesh services can be used at sites when running Ethernet cable to a location is inconvenient, expensive or impossible. Note that power must be available at the location where the Mesh AP is installed.

### Enhancements to Mesh Services

Multihop is now available when configuring Mesh Services. The system can support up to 16 Mesh Portals with each Mesh Portal supporting a 6 Mesh AP fan-out with a depth of 2 Mesh APs. Also, a single MP can perform two roles: Mesh Portal and Mesh MP.

Mesh Services reliability is improved by adding the following enhancements:

- Improved transmission of station session record.
- Ability to manage link loss between Mesh Portals and Mesh APs.
- Improved management of duplicate messages for SSR updates from multiple Mesh APs.

Mesh portal selection has improved by scanning for Mesh Link SSIDs and sorting them by RSSI values. The Mesh AP establishes a link using the RSSI values in descending order. If all attempts fail, the Mesh AP scans from the beginning of the table. After 60 seconds and no link is established, the Mesh AP reboots.

If the Mesh Link is using a DFS channel, then the Mesh Link has a timeout of 140 seconds to allow for DFS channel assessment. Mesh Portal selection is improved by scanning for Mesh Link SSIDs and sorting them by RSSI values. The Mesh AP establishes a link using RSSI values in descending order. If all attempts fail, the Mesh AP scans from the beginning of the table. After 60 seconds and no link is established, the Mesh AP reboots.

If the Mesh Link is using a DFS channel, then the Mesh Link has a timeout of 140 seconds to allow for DFS channel assessment.

**Figure 13–1** illustrates how a client can connect to a network using WLAN mesh services.

Configuring WLAN Mesh Services

## Configuring the Service Profile for Mesh Services

You configure the Mesh Portal AP to beacon the mesh services SSID. To do this, create a service profile and enable mesh services using the following commands:

```
MX# set service-profile mesh-service-profile ssid-name mesh-ssid
MX# set service-profile mesh-service-profile mesh mode {enable | disable}
```

The service profile can then be mapped to a radio profile that manages a radio on the Mesh Portal. Note that the radio profile mapped to the service profile cannot be configured to auto-tune power or channel settings.

To map the service profile to a radio profile, use the following command:

```
MX# set radio-profile mesh-radio-profile service-profile mesh-service-profile
```

Since auto-tune is enabled by default, you must disable it on the Mesh Portal using the following command:

```
MX# set radio-profile mesh-profile-name auto-tune channel-config disable
```

## Configuring Security

The secure connection between the Mesh AP and the Mesh Portal AP is established in a two-step process: 1) creation of an encrypted point-to-point link between the Mesh AP and the Mesh Portal AP, and2) authentication of the Mesh AP.

When the Mesh AP is booted, it searches for a beacon containing the configured mesh SSID. Once the Mesh AP locates a Mesh Portal AP with the mesh SSID, it associates with the Mesh Portal AP as a client device. The Mesh AP can then be authenticated by the MX.

To configure the Mesh AP for authentication, use the following commands:

```
set service-profile mesh-service-profile cipher-ccmp enable
set service-profile mesh-service-profile rsn-ie enable
set service-profile mesh-service-profile {psk-phrase pass-phrase | psk-raw raw-pass}
set service-profile mesh-service-profile auth-psk enable
set authentication mac ssid mesh-ssid * local
```

The or is the same one configured on the Mesh AP. Optionally, the fingerprint of the Mesh AP can be configured on the MX for additional security.

You can also configure last-resort authentication for clients accessing the Mesh APs using the following commands:

```
MX# set service-profile mesh-service-profile auth-dot1x disable
MX# set service-profile mesh-service-profile auth-fallthru last-resort
```

## Recommended Configuration Best Practices

The following recommendations provide the most stable mesh services on a wireless network:

- Dedicate one radio to client services and one radio to mesh services. Trapeze recommends that you dedicate the 802.11a radio (radio 2) to mesh services and the 802.11b radio (radio 1) to client services.
- Dedicate the Mesh Portal to mesh services if you anticipate a full client load through the Mesh MP.
- Limit the length of the mesh link to 3/8ths of a mile (1.09 km) or less if you have configured MSS 6.0.4 or earlier. Later versions of MSS support distances up to 1 mile (1.6 km) for Mesh Links.
- Enable local switching on the Mesh Portal and all Mesh MPs. Although local switching is not related to mesh services, configuring it may improve your throughput on the MP.
- . You can configure a mesh network with a mesh width of 10Mesh Portal APs and a mesh depth of 4 Mesh APs per Mesh Portal AP.

### Enabling Link Calibration Packets on the Mesh Portal MP

A Mesh Portal MP can be configured to emit to assist with positioning the Mesh AP. A link calibration packet is an unencrypted 802.11 management packet of type . When enabled on an MP, link calibration packets are sent at a rate of 5 per second.

The MP-620 is equipped with a connector to which an external RSSI meter can be attached during installation. When an RSSI meter is attached to an MP-620 and a calibration packet is received, the MP-620 emits a voltage to the RSSI meter proportional to the received signal strength of the packet. This can aid in positioning the MP-620 where it has a strong signal to the Mesh Portal AP.

To enable link calibration packets on an MP radio, use the following command:

```
set ap num radio num link-calibration mode {enable | disable}
```

Only one radio on an MP can be configured to send link calibration packets. Link calibration packets are intended to be used only during installation of MPs; they are not intended to be enabled on a continual basis.

### Deploying the Mesh AP

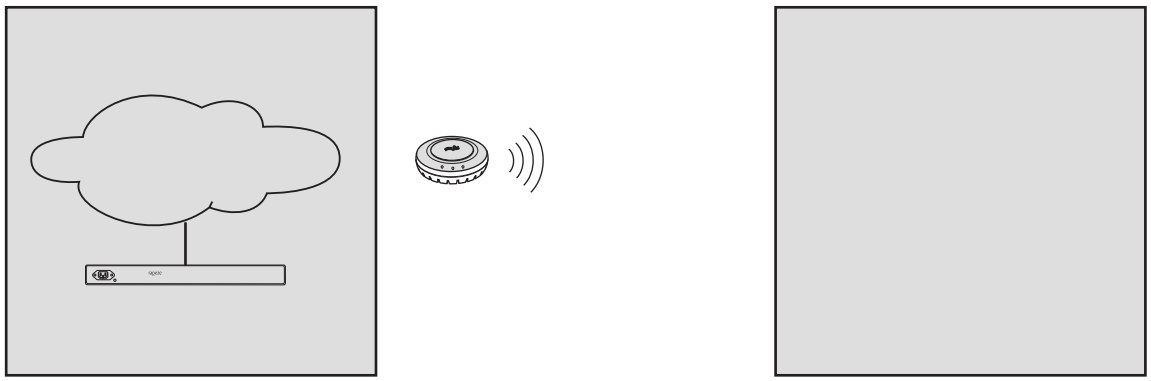
After you have configured the Mesh AP with mesh services settings, detach the AP from the wired network and place it in the desired location. The Mesh Portal AP must be within radio range of the Mesh AP.

## Configuring Wireless Bridging

You can use WLAN mesh services in a wireless bridge configuration, implementing MPs as bridge endpoints in a transparent Layer 2 bridge. Configuring a wireless bridge to connect two sites provides an alternative to installing Ethernet cable to provide bridge functionality.

A typical application of wireless bridging is to provide network connectivity between two buildings using a wireless link, as shown in Figure 2.

**Figure 13–2. Wireless Bridging**



The wireless bridge is established between a Mesh Portal AP and an associated Mesh AP. The bridged data packets are present on the Ethernet interfaces of the two MPs.

A Mesh Portal AP deployed as a bridge endpoint can support up to five Mesh APs configured as bridge endpoints. A Mesh AP serving as a bridge endpoint picks up packets from the wired port and transfers them to the other bridge endpoint. A simple source/destination learning mechanism is used to avoid forwarding packets across the bridge unnecessarily.

To enable wireless bridging for a service profile, use the following command:

```
set service-profile mesh-service-profile bridging {enable | disable}
```

When wireless bridging is enabled for a service profile, the MPs with the applied service profile are bridge peers. When a Mesh AP associates with a Mesh Portal AP through this service profile, the Mesh Portal AP automatically configures the Mesh AP to operate in bridge mode.

The **show service-profile** command indicates if bridging is enabled for the service profile.

## Displaying WLAN Mesh Services Information

The **show ap status verbose** command indicates which MPs are Mesh APs and which are Mesh Portal MPs. For example:

```
MX# show ap status
 otal number of entries: 120
Operational: 1, Image Downloading: 0,  nknown: 119, Other: 0
Flags: o = operational, b = booting, d = image downloading
       c = configuring, f = configuration failed
       a = auto AP, m = mesh AP, p = mesh portal
       i = insecure, e = encrypted, u = unencrypt
AP  Flag IP Address      Model     MAC Address       Radio1 Radio2  ptime
--- ---- --------------- --------- ----------------- ------ ------ ------
  7 om-u                MP-422    00:0b:0e:00:ca:c0 D 1/1  D56/1  19h47m
```

The show ap status command displays the mesh services attributes for an MP and the associated BSSID of the Mesh Portal. For example:

```
MX# show ap status verbose
AP: 1, IP-addr: 10.8.255.10 (vlan 'corp'), AP model: mp-422,
        manufacturer:  rapeze, name: AP01
================================================
State:     operational (not encrypt)
CP  info:  Atheros:MIPS32 speed=220000000 Hz version=AR5312, ram=16777216
                s/n=111111 hw_rev=n/a
 ptime:    0 hours, 0 minutes, 11 seconds
 plink BSSID: 00:0b:0e:17:bb:00

Radio 1 type: 802.11g, state: configure succeed [Enabled] (802.11b protect)
      operational channel: 6 (Auto) operational power: 18
      bssid1: 00:0b:0e:fd:fd:cc, ssid: public
      RFID Reports: Inactive
      Antenna Link Calibration: Enabled

Radio 2 type: 802.11a, state: configure succeed [Enabled]
      operational channel: 36 operational power: 17
      bssid1: 00:0b:0e:fd:fd:cd, ssid: mesh-ssid (mesh)
```

The ﻉ eﻉ ﻉ command displays information about the links an MP has to Mesh APs and Mesh Portal APs.

```
MX# show ap mesh-links 1
AP: 1 IP-addr: 1.1.1.3
```

```
Operational Mode: Mesh-Portal
Bridging:Enabled

MX# show ap mesh-links 2
AP:2 IP-addr: 1.1.1.4
Operational Mode: Mesh AP
Bridging: Enabled

 plink Mesh Portal: 2049 (54 Mbps)
-------------------------------------------------
             packets           bytes
 X:             307           44279
RX:             315          215046

 plink Mesh Portal Candidate AP's (* - Current  plink Mesh Portal)
Radio Mesh Portal MAC RSSI SSID
-------------------------------
*1 00:0b:0e:41:2d:c0 -42 mesh_services
```

Use the **a b - a** command to display information about a Mesh AP:

```
MX# show ap boot-configuration 7

Static Boot Configuration
AP: 7

IP Address:  Disabled
VLAN  ag:    Disabled
Switch:      Disabled

Mesh:        Enabled

IP Address:
Netmask:
Gateway:
VLAN  ag:
Switch IP:
Switch Name:
DNS IP:
Mesh SSID:    mesh_services
Mesh PSK:     f06040b72104861a31611a854a5430dedf1c6f6d267b5e69cb13677b1a3fb93a
```

(For information about the fields in the output, see the .)

14

# Managing 802.1X on the MX

Certain settings for IEEE 802.1X sessions on the MX are enabled by default. For best results, change the settings only if you are aware of a problem with the MX 802.1X performance. For settings that you can reset with a **clear** command, MSS reverts to the default value.

See **"Managing WEP Keys" on page 14–2** for information about changing the settings for Wired-Equivalent Privacy protocol (WEP) key rotation (rekeying).

## Managing 802.1X on Wired Authentication Ports

A wired authentication port is an Ethernet port with 802.1X authentication enabled for access control. Like wireless users, users connected to an MX by Ethernet wire can be authenticated before authorizing use of the network. One difference between a wired authenticated user and a authenticated user is that data for wired users is not encrypted after the users are authenticated.

By default, 802.1X authentication is enabled for wired authenticated ports, but you can disable it. You can also set the port to unconditionally authorize, or unconditionally reject, all users.

### Enabling and Disabling 802.1X Globally

The following command globally enables or disables 802.1X authentication on all wired

Similarly, the following command forces port 12 to unconditionally reject any 802.1X attempts with an EAP failure message:

```
MX# set dot1x port-control forceunauth 12
success: authcontrol for 12 is set to FORCE- NA  H.
```

The **set dot1x port-control** command is overridden by the **set dot1x authcontrol** command. The **clear dot1x port-control** command returns port control to the default **auto** value.

Type the following command to reset port control for all wired authentication ports:

```
MX# clear dot1x port-control
success: change accepted.
```

# Managing 802.1X Encryption Keys

By default, the MX sends encryption key information to a wireless supplicant (client) in an Extensible Authentication Protocol over LAN (EAPoL) packet after authentication is successful. You can disable this feature or change the time interval for key transmission.

The Wired-Equivalent Privacy protocol (WEP) keys used by MSS on MPs for broadcast communication on a VLAN are automatically rotated (rekeyed) every 30 minutes to maintain secure packet transmission. You can disable WEP key rotation for debugging purposes, or change the rotation interval.

## Enabling 802.1X Key Transmission

The following command enables or disables the transmission of key information to the supplicant (client) in EAPoL key messages, after authentication:

```
set dot1x key-tx {enable | disable}
```

Key transmission is enabled by default.

The MX switch sends EAPoL key messages after successfully authenticating the supplicant (client) and receiving authorization attributes for the client. If the client is using dynamic WEP, the EAPoL Key messages are sent immediately after authorization.

Type the following command to reenable key transmission:

```
MX# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

## Configuring 802.1X Key Transmission Time Intervals

The following command sets the number of seconds the MX waits before retransmitting an EAPoL packet of key information:

```
set dot1x tx-period seconds
```

The default is 5 seconds. The range for the retransmission interval is from 1 to 65,535 seconds. For example, type the following command to set the retransmission interval to 300 seconds:

```
MX# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

Type the following command to reset the retransmission interval to the 5-second default:

```
MX# clear dot1x tx-period
success: change accepted.
```

## Managing WEP Keys

Wired-Equivalent Privacy (WEP) is part of the system security of 802.1X, and MSS uses WEP to provide confidentiality to packets as sent over the wireless network. WEP operates on the MP.

WEP uses a secret key shared between the communicators. WEP rekeying increases the security of the network, and new unicast keys are generated every time a client performs 802.1X authentication.

The rekeying process can be performed automatically on a periodic basis. By setting the Session-Timeout RADIUS attribute, the reauthentication is transparent to the client, who is unaware that reauthentication is occurring. A good value for Session-Timeout is 30 minutes.

WEP broadcast rekeying causes the broadcast and multicast keys for WEP to be rotated every WEP rekey period for each radio to each connected VLAN. The MX generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages. WEP keys are case-insensitive.

Use the **set dot1x wep-rekey** and the **set dot1x wep-rekey-period** commands to enable WEP key rotation and configure the time interval for WEP key rotation.

### Configuring 802.1X WEP Rekeying

WEP rekeying is enabled by default on the MX. Disable WEP rekeying only if you need to debug your 802.1X network.

Use the following command to disable WEP rekeying for broadcast and multicast keys:

```
MX# set dot1x wep-rekey disable
success: wep rekeying disabled
```


To reenable WEP rekeying, type the following command:

```
MX# set dot1x wep-rekey enable
success: wep rekeying enabled
```

### Configuring the Interval for WEP Rekeying

The following command sets the interval for rotating the WEP broadcast and multicast keys:

`set dot1x wep-rekey-period` *`seconds`*

The default is 1800 seconds (30 minutes). You can set the interval from 30 to 1,641,600 seconds (19 days). For example, type the following command to set the WEP-rekey period to 900 seconds:

```
MX# set dot1x wep-rekey-period 900
success: dot1x wep-rekey-period set to 900
```

## Setting EAP Retransmission Attempts

The following command sets the maximum number of times the MX retransmits an 802.1X-encapsulated EAP request to the supplicant (client) before it times out the authentication session:

`set dot1x max-req` *`number-of-retransmissions`*

The default number of retransmissions is 2. You can specify from 0 to 10 retransmit attempts. For example, type the following command to set the maximum number of retransmission attempts to 3:

```
MX# set dot1x max-req 3
success: dot1x max request set to 3.
```

To reset the number of retransmission attempts to the default setting, type the following command:

```
MX# clear dot1x max-req
success: change accepted.
```


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.

The interval of time before retransmitting an 802.1X-encapsulated EAP request to the supplicant is the same number of seconds as one of the following timeouts:

- Supplicant timeout (configured by the **set dot1x timeout supplicant** command)
- RADIUS session-timeout attribute

If both timeouts are set, MSS uses the shorter of the two. If the RADIUS session-timeout attribute is not set, MSS uses the timeout specified by the **set dot1x timeout supplicant** command, by default 30 seconds.

# Managing 802.1X Client Reauthentication

Reauthentication of 802.1X wireless clients is enabled on the MX by default. By default, the MX waits 3600 seconds (1 hour) between authentication attempts. You can disable reauthentication or change the defaults.


You also can use the RADIUS session-timeou

## Enabling and Disabling 802.1X Reauthentication

The following command enables or disables the reauthentication of supplicants (clients) by the MX:

```
set dot1x reauth {enable | disable}
```

Reauthentication is enabled by default.

Type the following command to reenable reauthentication of clients:

```
MX# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

## Setting the Maximum Number of 802.1X Reauthentication Attempts

The following command sets the number of reauthentication attempts that the MX makes before the supplicant (client) becomes unauthorized:

```
set dot1x reauth-max number-of-attempts
```

The default number of reauthentication attempts is 2. You can specify from 1 to 10 attempts. For example, type the following command to set the number of authentication attempts to 8:

```
MX# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

Type the following command to reset the maximum number of reauthorization attempts to the default:

```
MX# clear dot1x reauth-max
success: change accepted.
```


### Setting the 802.1X Reauthentication Period

The following command configures the number of seconds before attempting reauthentication:

```
set dot1x reauth-period seconds
```

The default is 3600 seconds (1 hour). The range is from 60 to 1,641,600 seconds (19 days). This value can be overridden by user authorization parameters.

MSS reauthenticates dynamic WEP clients based on the reauthentication timer. MSS also reauthenticates WPA clients if the clients use the WEP-40 or WEP-104 cipher. For each dynamic WEP client or WPA client using a WEP cipher, the reauthentication timer is set to the lesser of the global setting or the value returned by the AAA server with the rest of the authorization attributes for the client.

For example, type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
MX# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

Type the following command to reset the default timeout period:

```
MX# clear dot1x reauth-period
success: change accepted.
```

### Setting the Bonded Authentication Period

The following command sets the Bonded Auth™ (bonded authentication) period, the number of seconds MSS retains session information for an authenticated computer while waiting for the 802.1X client on the computer to start (re)authentication for the user.

Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

To set the Bonded Auth period, use the following command:

```
set dot1x bonded-period seconds
```

The Bonded Auth period applies only to 802.1X authentication rules that contain the **bonded** option.

To reset the Bonded Auth period to the default value, use the following command:

```
clear dot1x max-req
```

(For more information about Bonded Auth, see **“Binding User Authentication to Computer Authentication” on page 11–11**.)

## Managing Other Timers

By default, the MX waits 60 seconds before responding to a client whose authentication failed, and times out a request to a RADIUS server or an authentication session with a client after 30 seconds. You can modify these defaults.

## Setting the 802.1X Quiet Period

## Viewd1X Statistics

Type the followd command to display 802.1X st atistics about connectiauthenticating:

```
MX# show dot1x stats
        802.1X statistic                value
        ----------------                -----
        Enters Connecting:              709
        Logoffs While Connecting:       112
        Enters Authenticating:          467
        Success While Authenticating:   0
         imeouts 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
```

For information about the fields in the output, see the
.

# Configuring User Encryption

Mobility System Software (MSS) encrypts wireless user traffic for all authenticated users on an encrypted SSID and then an authorized VLAN. MSS supports the following types of encryption for wireless user traffic:

- 802.11i
- Wi-Fi Protected Access (WPA)
- Non-WPA dynamic Wired Equivalent Privacy (WEP)
- Non-WPA static WEP

WPA and 802.11i provide stronger security than WEP. (802.11i uses
, and is sometimes called .)

To use WPA or RSN, a cliecNrbusts(u)5upprt (th)]TJ-1.144 0 TD.0011 Tc-.0018 Tw[(( prtocol. Fe)-6-6(y)1.1r n

- Wired Equivalent Privacy (WEP) with 104-bi

**Figure 15–3. WPA Encryption with TKIP and WEP**

## TKIP Countermeasures

WPA access points and clients verify the integrity of a wireless frame received on the network by generating a keyed message integrity check (MIC). The MIC used with TKIP provides a holddown mechanism to protect the network against tampering.

- If the recalculated MIC matches the MIC rece

- When the countermeasures timer expires, the access point allows associations and

- If a client wants to authenticate with dynamic WEP, MSS uses 802.1X to authenticate the client if either the WEP40 or WEP104 cipher suite is enabled for WPA.
- If a client wants to authenticate using static WEP, the radio checks for the static WEP key presented by the client. If the keys match, MSS authenticates the client. Because the WEP key is static, MSS does not use 802.1X to authenticate the client.

To allow a non-WPA client with dynamic WEP to be authenticated by a radio with WPA IE enabled, enable the WEP40 or WEP104 cipher suite in the service profile for the SSID. To prevent non-WPA clients with dynamic WEP from authenticating, do not enable the WEP40 or WEP104 cipher suite in the service profile.

To allow a client that uses static WEP to be authenticated, configure the same WEP keys on the client and the service profile.

**Table 15– 2** lists the encryption support for WPA and non-WPA clients.

**Table 15– 2. Encryption Support for WPA and Non-WPA Clients**

| MSS Encryption Type | Client Encryption Type | | | | | |
|---|---|---|---|---|---|---|
| | **WPA—CCMP** | **WPA—TKIP** | **WPA—WEP40** | **WPA—WEP104** | **Dynamic WEP** | **Static WEP** |
| **WPA—CCMP** | Supported | | | | | |
| **WPA—TKIP** | | Supported | | | | |
| **WPA—WEP40** | | | Supported | | Supported | |
| **WPA—WEP104** | | | | Supported | Supported | |
| **Dynamic WEP** | | | | | Supported | |
| **Static WEP** | | | | | | Supported |

## Configuring WPA

To configure MP access point radios to support WPA:

1. Create a service profile for each SSID that supports WPA clients.
2. Enable the WPA IE in the service profile.
3. Enable the cipher suites to support in the service profile. (TKIP is enabled by default.) Optionally, you also can change the countermeasures timer value for TKIP.
4. Map the service profile to the radio profile that controls IEEE settings for the radios.
5. Assign the radio profile to the radios and enable the radios.

If you plan to use PSK authentication, you also need to enable this authentication method and enter an ASCII passphrase or a hexadecimal (raw) key.

### Creating a Service Profile for WPA

Encryption parameters apply to all users who use the SSID configured by a service profile. To create a service profile, use the following command:

```
set service-profile profile-name
```

To create a new service profile named , type the following command:

```
MX# set service-profile wpa
success: change accepted.
```

## Enabling WPA

To enable WPA, you must enable the WPA information element (IE) in the service profile. To enable the WPA IE, use the following command:

```
set service-profile profile-name wpa-ie {enable | disable}
```

To enable WPA in service profile , type the following command:

```
MX# set service-profile wpa wpa-ie enable
success: change accepted.
```

## Specifying the WPA Cipher Suites

To use WPA, at least one cipher suite must be enab

To enable PSK authentication, use the following command:

```
set service-profile profile-name auth-psk {enable | disable}
```

To enable PSK authentication in service profile , type the following command:

```
MX# set service-profile wpa auth-psk enable
success: change accepted.
```

### Configuring a Global PSK Passphra

```
Custom logout web-page:                  Custom agent-directory:
Static COS:                        no    COS:                                0
CAC mode:                        none    CAC sessions:                      14
 ser idle timeout:                180    Idle client probing:              yes
Keep initial vlan:                 no    Web Portal Session  imeout:         5
Web Portal ACL:
WEP Key 1 value:                <none>   WEP Key 2 value:                <none>
WEP Key 3 value:                <none>   WEP Key 4 value:                <none>
WEP  nicast Index:                   1   WEP Multicast Index:                 1
Shared Key Auth:                    NO
WPA enabled:
    ciphers: cipher-tkip, cipher-wep40
    authentication: 802.1X
     KIP countermeasures time: 30000ms
11a beacon rate:                   6.0   multicast rate:                   A  O
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:                   A  O
11b mandatory rate: 1.0,2.0 standard rates: 5.5,11.0
11g beacon rate:                   2.0   multicast rate:                   A  O
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
```

The WPA settings appear at the bottom of the output.

o

## Assigning the Service Profile to Radios and Enabling the Radios

After you configure WPA settings in a service profile, you can map the service profile to a radio profile, assign the radio profile to radios, and enable the radios to activate the settings.

To map a service profile to a radio profile, use the following command:

`set radio-profile` *`profile-name`* `service-profile` *`profile-name`*

To assign a radio profile to radios and enable the radios, use the following command:

`set ap port-list radio {1 | 2} radio-profile` *`profile-name`* `mode`

# Configuring RSN (802.11i)

Robust Security Network (RSN) provides 802.11i support. RSN uses AES encryption.

You can configure a service profile to support RSN clients exclusively, or to support RSN with WPA clients, or even RSN, WPA and WEP clients.

The configuration tasks for a service profile to use RSN are similar to the tasks for WPA:

1. Create a service profile for each SSID that supports RSN clients.
2. Enable the RSN IE in the service profile.
3. Enable the cipher suites to support in the service profile. (TKIP is enabled by default.) Optionally, you also can change the countermeasures timer value for TKIP.
4. Map the service profile to the radio profile that controls IEEE settings for the radios.
5. Assign the radio profile to the radios and enable the radios.

If you plan to use PSK authentication, you also need to enable this authentication method and enter an ASCII passphrase or a hexadecimal (raw) key.

## Creating a Service Profile for RSN

Encryption parameters apply to all users who use the SSID configured by a service profile. To create a service profile, use the following command:

```
set service-profile name
```

To create a new service profile named , type the following command:

```
MX# set service-profile rsn
success: change accepted.
```

## Enabling RSN

To enable RSN, you must enable the RSN information element (IE) in the service profile. To enable the RSN IE, use the following command:

```
set service-profile name rsn-ie {enable | disable}
```

To enable RSN in service profile , type the following command:

```
MX# set service-profile rsn rsn-ie enable
success: change accepted.
```

## Specifying the RSN Cipher Suites

To use RSN, at least one cipher suite must be end.

## Enabling WPA with TKIP

The following example shows how to configure MSS to provide authentication and TKIP encryption for 801.X WPA clients. This example assumes that pass-through authentication is used for all users. A RADIUS server group performs all authentication and authorization for the users.

**1.** Create an authentication rule that sends all 802.1X users of SSID in the domain to the server group for authentication. Type the following command:

```
MX# set authentication dot1x ssid mycorp EXAMPLE\* pass-through shorebirds
```

**2.** Create a service profile named for the SSID. Type the following command:

```
MX# set service-profile wpa
success: change accepted.
```

**3.** Set the SSID in the service profile to . Type the following command:

```
MX# set service-profile wpa ssid-name mycorp
success: change accepted.
```

**4.** Enable WPA in service profile . Type the following command:

```
MX# set service-profile wpa wpa-ie enable
success: change accepted.
```

TKIP is already enabled by default when WPA is enabled.

**5.** Display the service profile to verify the changes. Type the following command:

```
MX# show service-profile sp1
ssid-name:                      mycorp   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
CAC mode:                         none   CAC sessions:                      14
 ser idle timeout:                 180   Idle client probing:              yes
Keep initial vlan:                  no   Web Portal Session  imeout:         5
Web Portal ACL:
WEP Key 1 value:                <none>   WEP Key 2 value:                <none>
WEP Key 3 value:                <none>   WEP Key 4 value:                <none>
WEP  nicast Index:                   1   WEP Multicast Index:                1
Shared Key Auth:                    NO
WPA enabled:
    ciphers: cipher-tkip
    authentication: 802.1X
     KIP countermeasures time: 60000ms
...
```

**6.** Map service profile to radio profile . Type the following commands:

```
MX# set radio-profile rp1 service-profile wpa
success: change accepted.
```

**7.** Apply radio profile to radio 1 on port 5 and to radios 1 and 2 on port 11, enable the radios, and verify the configuration changes. Type the following commands:

```
MX# set ap 5,11 radio 1 radio-profile rp1 mode enable
success: change accepted.
MX# set ap 11 radio 2 radio-profile rp1 mode enable
success: change accepted.
MX# show ap config
Port  5: AP model: mp-241, POE:  enable, bias: high, name: MP05
           boot-download-enable: YES
           force-image-download: YES
  Radio 1: type: 802.11a, mode:  enabled, channel: 36
```

```
  tx pwr:  1, profile: rp1
  auto-tune max-power: default,
Port  11: AP model: mp-252, POE:  enable, bias: high, name: MP11
          boot-download-enable: YES
          force-image-download: YES
  Radio 1: type: 802.11g, mode:  enabled, channel: 6
  tx pwr:  1, profile: rp1
  auto-tune max-power: default
  Radio 2: type: 802.11a, mode: enabled, channel: 36
  tx pwr:  1, profile: rp1
  auto-tune max-power: default
```

**8.** Save the configuration. Type the following command:

```
MX# save config
success: configuration saved.
```

## Enabling Dynamic WEP in a WPA Network

The following example shows how to configure MSS to provide authentication and encryption for 801.X dynamic WEP clients, and for 801.X WPA clients using TKIP. Th.4(e)2uune nexgampi. ta1t troughe aut1etic a1tioniso conigue(d foralM)]TJ2215068 0 TD.0081 Tc-.0005 Tw[ls uers. (Thg )-6(c(mmnds. )-6a ThgW.E4.6Ps cipns61r6(i)-13(ca1)498ttion andoeancry1do6 non- WPA lge(in sca.8)6(t)Xn SSID t

```
Shared Key Auth:                    NO
WPA enabled:
    ciphers: cipher-tkip, cipher-wep40
    authentication: 802.1X
     KIP countermeasures time: 60000ms
...
```

**7.** Map service profile to radio profile . Type the following commands:

```
MX# set radio-profile rp2 service-profile wpa-wep
success: change accepted.
```

**8.** Apply radio profile to radio 1 on port 5 and to radios 1 and 2 on port 11, enable the radios,

```
Server                   Addr           Ports    /o  ries Dead State
-------------------------------------------------------------------

Server groups

Web Portal:
enabled

set authentication mac ssid voice * local

mac-usergroup wpa-for-mac
   vlan-name = blue

mac-user aa:bb:cc:dd:ee:ff
   Group = wpa-for-mac

mac-user a1:b1:c1:d1:e1:f1
   Group = wpa-for-mac
```

**5.** Create a service profile named for SSID voice. Type the following command:

```
MX# set service-profile wpa-wep-for-mac
success: change accepted.
```

**6.** Set the SSID in the service profile to . Type the following command:

```
MX# set service-profile wpa-wep-for-mac ssid-name voice
success: change accepted.
```

**7.** Enable WPA in service profile . Type the f4cpnofgcomml4c54(n)-1nd:

```
WPA enabled:
    ciphers: cipher-tkip, cipher-wep40
    authentication: pre-shared key
     KIP countermeasures time: 60000ms
    pre-shared-key: 92f99cd49e186cadee13fda7b2a2bac78975
         a5723a4a6b31b5b5395d6b001dbe
```

**12.** Map service profile to radio profile . Type the following commands:

```
MX# set radio-profile rp3 service-profile wpa-wep-for-mac
success: change accepted.
```

**13.** Apply radio profile to radio 1 on port 4 and to radios 1 and 2 on port 6 and enable the radios, and verify the configuration changes. Type the following commands:

```
MX# set ap 4,6 radio 1 radio-profile rp3 mode enable
success: change accepted.
MX# set ap 6 radio 2 radio-profile rp3 mode enable
success: change accepted.
MX# show ap config
Port  4: AP model: MP-241, POE:  enable, bias: high, name: MP04
           boot-download-enable: YES
           force-image-download: YES
  Radio 1: type: 802.11a, mode:  enabled, channel: 36
  tx pwr:  1, profile: rp3
  auto-tune max-power: default
Port  6: AP model: mp-252, POE:  enable, bias: high, name: MP06
           boot-download-enable: YES
           force-image-download: YES
  Radio 1: type: 802.11g, mode:  enabled, channel: 6
  tx pwr:  1, profile: rp3
  auto-tune max-power: default
  Radio 2: type: 802.11a, mode: enabled, channel: 36
  tx pwr:  1, profile: rp3
```

# Configuring and Managing Mobility Domains

A Mobility Domain is a system of MX switches and MPs working together to support roaming wireless clients. Tunnels and virtual ports between the MX switches in a Mobility Domain allow users to roam without any disruption to network connectivity.


## About the Mobility Domain Feature

A Mobility Domain enables users to roam geographically across the system while maintaining data sessions and VLAN or subnet membership, including IP address, regardless of connectivity to the network backbone. As users move from one area of a building or campus to another, client associations with servers or other resources appears the same.

When users access an MX in a Mobility Domain, they become members of the VLAN designated through their authorized identity. If a native VLAN is not present on the accessed MX, the MX forms a tunnel to an MX in the Mobility Domain that includes the native VLAN.

In a Mobility Domain, one MX acts as a seed device, and distributes information to the MX switches defined in the Mobility Domain. Otherwise, the seed MX operates as any other Mobility Domain member.

## Smart Mobile Virtual Controller Cluster

Trapeze Networks uses innovative clustering technology between MX switches to ensure mobility across an entire wireless network. With clustering, you can effortlessly create logical groups of MX switches and MPs, which proactively share network and user information for hitless failover support. You can also create a single point of configuration for small and large WLAN deployments to reduce the cost of installation and network management. Adding MXs and MPs is seamless and does not require an interruption of connectivity in your existing network.

Smart Mobile Virtual Controller Clustering provides distributed network intelligence that enables fast, transparent failover to overcome network and device interruptions and provides a means of central configuration and distribution for MXs and MPs on the network.

The features of cluster configuration include the following:

- 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.

To configure Virtual Controller Cluster services to your network, see **“Smart Mobile Virtual Controller Cluster Configuration” on page 17–4**.

# Configuring a Mobility Domain

The MX switches in a Mobility Domain use a system IP address for Mobility Domain communication. To support the services of the Mobility Domain, the MX system IP address requires basic IP connectivity to the system IP address of every other MX. (For information about setting the system IP address for the MX switch, see the
.)

```
set mobility-domain mode member seed-ip ip-addr
```

This command configures the IP destination address used to communicate with the seed MX.

For example, the following command configures the current MX as a member of the Mobility Domain whose seed is 192.168.253.6:

```
MX# set mobility-domain mode member seed-ip 192.168.253.6
success: change accepted.
```

This command sets the MX as a member of the Mobility Domain defined on the seed device at the identified address. If the MX is currently part of another Mobility Domain or using another seed MX, this command overwrites that configuration. After you enter this command, the member MX obtains a new list of members from the new seed IP address.

## Configuring Mobility Domain Seed Redundancy

You can optionally specify a in a Mobility Domain. The secondary seed provides redundancy for the primary seed switch in the Mobility Domain. If the primary seed becomes unavailable, the secondary seed assumes the role of the seed MX. This allows the Mobility Domain to continue functioning if the primary seed becomes unavailable.

Specifying a secondary seed for a Mobility Domain is useful since it eliminates the single point of failure if connectivity to the seed MX is lost.

When the primary seed switch fails, the remaining members form a Mobility Domain, with the secondary seed taking over as the primary seed MX.

- (o)b=(X)freasguresare( )-6(ineffve)-480(cg )-6(en the prin)]TJ02.4978 0 TD.0325 Tc-.0402 Tw[(ary43.5( )-6(s volie(.)]TJ -1.2650 -1.6024 TD.0009 Tc-.0016 Tw[(

```
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
```

### Displaying the Mobility Domain Configuration

To view the configuration of the Mobility Domain, use the **show mobility-domain config** command on either the seed or a nonseed member.

To view Mobility Domain configuration on the seed:

```
MX-20#show mobility-domain config
 his MX is the seed for domain Pleasanton.
192.168.12.7 is a member
192.168.15.5 is a member
```

To view Mobility Domain configuration on a member:

```
MX-20#show mobility-domain config
 his MX is a member, with seed 192.168.14.6
```

### Clearing a Mobility Domain from an MX

You can clear all Mobility Domain configuration from an MX.

You might want to clear the Mobility Domain information to change an MX from one Mobility Domain to another, or to remove an MX from the Mobility Domain. To clear the Mobility Domain, type the following command:

```
MX-20#clear mobility-domain
success: change accepted
```

### Clearing a Mobility Domain Member from a Seed

You can remove individual members from the Mobility Domain on the seed MX. To remove a specific member of the Mobility Domain, type the following command:

```
clear mobility-domain member ip-addr
```

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.

## Smart Mobile Virtual Controller Cluster Configuration

### Virtual Controller Cluster Configuration Terminology

- Domain configuration – Wireless parameters in the configuration file, including radio profiles, service profiles, AP configuration, and more. The Domain configuration is typically duplicated among more than one MX in a cluster.
- Configuration Cluster – The cluster subset of MXs in a Mobility Domain that share a domain configuration.
- Primary AP Manager (PAM) – The MX in the cluster responsible for actively managing APs that receive configuration information from the PAM.
- Secondary AP Manager (SAM) – The MX in the cluster acting as the hot standby for an AP.

### Centralized Configuration Using Virtual Controller Cluster Mode

- Cluster mode is a subset of a Mobility Domain.
- A predetermined set of configuration parameters are distributed from the primary seed to members of the cluster in a load balanced manner. The MP parameters are then distributed to the MPs on each MX.
- A member of a configuration cluster does not have a local copy of the domain configuration unless it is the primary or secondary seed.
  - An MX cannot boot an AP without network connectivity to the primary or secondary seed.

  - The domain configuration is created and managed by the active seed.
  - The secondary seed provides redundancy for configuration management to the primary seed.
  - The primary seed takes precedence over the secondary seed if there are conflicting configurations between them. The only exception is if you explicitly override the configuration.
  - Changes to the secondary seed are not allowed while the primary seed is active on the network.
- Adding more MXs to the cluster to increase MP booting capacity is seamless and requires no configuration changes to more than one MX in the cluster.
- Configuration changes for MXs can only be performed on the primary seed of the Mobility Domain, or the secondary seed if one is configured and the primary seed is unavailable.

## Autodistribution of MPs on the Virtual Controller Cluster

- Load balancing of MPs is supported across the cluster without any explicit configuration.
- The maximum number of configured MPs on the cluster is restricted by the maximum number of configured MPs on the primary or secondary seed. Larger capacity MXs should be used for larger deployments of MPs.
- Client session states are shared among MXs in the cluster configuration.

## “Hitless” Failover with Virtual Controller Cluster Configuration

-

```
MX_PS# set cluster mode enable
success:change accepted
```

On the secondary seed for the Mobility Domain, enter the following 2 8.64 refQq1 i 0 -6.6t0

The following commands can only be executed on the active seed within the cluster configuration:

```
MX# set ap
MX# set service-profile
MX# set radio-profile
MX# set security acl map name ap aplist {in | out}
MX# set location policy
MX# set mobility-profile
MX# set vlan-profile
MX# set rfdetect
MX# set system countrycode
MX# set load-balancing
MX# set qos-profile
MX# set snoop
```

### Other Virtual Controller Cluster Configuration Parameters

The following configuration parameters are also shared as part of the cluster configuration:

- ACLs – are implemented as follows:
  - ACLs that refer to an AP must be configured on the seed MX.
  - ACLs defined on a seed MX are shared with members.
  - ACL mapping to ports, VLANs, and vports can be defined on the member MXs for locally defined ACLs.
  - If there are conflicting ACL names, the local ACL takes precedence and the incident is logged to the event log.
- Mobility profiles – have the following configuration constraints:
  - Mobility profiles must be configured on the Primary seed.
  - Mobility profiles that reference ports are not accepted by the configuration.
- Location policies – can be configured as follows:
  - Must be configured on the seed MX.
  - Profiles with port references are not allowed.
- QoS profiles

## Configuring MX-MX Security

You can enhance security on your network by enabling MX-MX security. MX-MX security encrypts management traffic exchanged by MX switches in a Mobility Domain.

When MX-MX security is enabled, management traffic among MX switches in the Mobility Domain is encrypted using AES. The keying material is dynamically generated for each session and passed among switches using configured public keys.

To configure MX-MX security:

1. Set Mobility Domain security on each MX to **required**. The default setting is **none**. MX-MX security can be disabled or enabled on a Mobility Domain basis. The feature must have the same setting (**required** or **none**) on all switches in the Mobility Domain. Use the following command on the seed and on each member to enable MX-MX security:

```
set domain security required
```

   This command also creates a certificate.

2. On the seed and on each member, generate a private key. Use the following command:

```
crypto generate key domain 128
```

3. On the Mobility Domain seed, display the generated key by using the following command:

```
show crypto key domain
```

   Copy the key in order to use it on other mobility domain members.

4. On the Mobility Domain seed, specify the public key for each member. Use the following command:

```
set mobility-domain member ip-addr key hex-bytes
```

Specifies the key as 16 hexadecimal bytes, separated by colons. Here is an example:

```
91:3e:ef:48:76:ff:fc:8b:52:ef:58:04:1e:51:1e:25
```

5. On each member MX, specify the seed IP address and the public key. Use the following command:

```
set mobility-domain mode member seed-ip ip-addr key hex-bytes
```

This command does not need to be entered on the seed MX.

# Monitoring the VLANs and Tunnels in a Mobility Domain

Tunnels connect MX switches across a network. Tunnels are formed automatically in a Mobility Domain to extend a VLAN to the MX with an associated roaming station. A single tunnel can carry traffic for many users and many VLANs. The tunnel port can carry traffic for multiple VLANs by means of multiple .

MSS automatically adds virtual ports to VLANs as needed to preserve the associations of users to the correct subnet or broadcast domain as they roam across the Mobility Domain. Although tunnels are formed by IP between MX switches, the tunnels can carry user traffic of any protocol type.

MSS provides the following commands to display the roaming and tunneling of users within Mobility Domain groups:

- **show roaming station** (See **Displaying Roaming Stations**.)
- **show roaming vlan** (See **"Displaying Roaming VLANs and Affinities" on page 17–8**.)
- **show tunnel** (See **"Displaying Tunnel Information" on page 17–9**.)

## Displaying Roaming Stations

The command **show roaming station** displays a list of the stations roaming to the MX through a VLAN tunnel. To display roaming stations (clients), type the following command:

```
MX# show roaming station
 ser Name              Station Address   VLAN            State
---------------------- ----------------- --------------- -----
example\geetha         192.168.15.104    vlan-am          p
nh@example.com         192.168.15.1990   vlan-am          p
example\tamara         192.168.11.200    vlan-ds          p
example\jose           192.168.14.200    vlan-et          p
hh@example.com         192.168.15.194    vlan-am          p
```

(For more information about this command and the fields in the output, see the .)

## Displaying Roaming VLANs and Affinities

The command **show roaming vlan** displays all VLANs in the Mobility Domain, the MX switches configured for the VLANs, and the tunnel values configured on each MX.

The member MX that offers the requested VLAN reports the affinity number. If multiple MX switches have native attachments to the VLAN, the advertised affinity values attract tunneled traffic to a particular MX for that VLAN. A higher value represents a preferred connection to the VLAN. (For more information, see the .)

To display roaming VLANs, type the following command:

```
MX# show roaming vlan
VLAN             MX               Affinity
---------------- ---------------- --------
vlan-eng         192.168.12.7            5
```

```
vlan-fin          192.168.15.5          5
vlan-pm           192.168.15.5          5
vlan-wep          192.168.12.7          5
vlan-wep          192.168.15.5          5
```

(For more information about this command and the fields in the output, see the )

## Displaying Tunnel Information

The command **show tunnel** displays the tunnels hosted on the MX and distributes to a locally

68.12.7 .15.5 4 vlan-wep 168.192.168.12.7 .15.5 3 168

or more information about this command and the fields in the output, see the

If the client changes the encryption type or VLAN name, MSS might record a new session rather than a roamed session.

## Effects of Timers on Roaming

An unsuccessful roaming attempt might be caused by the following timers. You cannot configure either timer.

- **Grace period.** A disassociated session has a grace period of 5 seconds during which MSS can retrieve and forward the session history. After 5 seconds, MSS clears the session, and the accounting is stopped.
- **MAC address search.** If MSS cannot find the client MAC address in a Mobility Domain within 5 seconds, the session is treated as a new session rather than a roaming session.

In contrast, the 802.1X reauthentication timeout period has little effect on roaming. If the timeout expires, MSS performs 802.1X processing on the existing association. Accounting and roaming history are unaffected when reauth

**3.** For each member MX, configure the IP address to reach the seed MX. Type the following commands:

```
MX# set mobility-domain member seed-ip 192.168.253.21
```

**4.** Display the Mobility Domain status. Type the following command:

```
MX# show mobility-domain
Mobility Domain name:  sunflower
Member              State             Status
---------------     -------------     --------------
192.168.111.112     S A E_ P          MEMBER
192.168.253.11      S A E_ P          MEMBER
192.168.253.21      S A E_ P          SEED
```

**5.** To display the Mobility Domain configuration, type the following command:

```
MX# show mobility-domain config
 his MX is the seed for domain sunflower.
192.168.253.11 is a member
192.168.111.112 is a member
```

**6.** To display the MX switches that are hosting VLANs for roaming, type the following command:

```
MX# show roaming vlan
VLAN             MX              Affinity
---------------- --------------- --------
vlan-eng         192.168.12.7           5
vlan-fin         192.168.15.5           5
vlan-pm          192.168.15.5           5
vlan-wep         192.168.12.7           5
vlan-wep         192.168.15.5           5
```

**7.** To display active roaming tunnels, type the following command:

```
MX# show tunnel
VLAN             Local Address   Remote Address  State   Port  LVID  RVID
-------------- --------------- --------------- ------- ----- ----- -----
vlan-eng         192.168.12.7    192.168.15.5     P       1025   130  4096
vlan-eng         192.168.12.7    192.168.14.6     P       1024   130  4096
```

18

# Configuring Network Domains

## About the Network Domain Feature

A Network Domain allows functionality found in Mobility Domains to be extended over a multiple-site installation. A user configured to be on a VLAN at the home site can travel to a remote site, connect to the network, and placed in the native VLAN. To do this, the accessed MX forms a tunnel to an MX at the home site of a user.

**Figure 18–1**

**Figure 18–2. Connecting to a Remote VLAN in a Network Domain**


In this example, Bob establishes connectivity as follows:

1. Bob connects to the wireless network at the Corporate Office. The MX contacts the local Mobility Domain seed and finds that the VLAN configured for Bob, VLAN Red, does not exist in the Corporate Office Mobility Domain.
2. Unable to find VLAN Red in the local Mobility Domain, the MX then contacts the local Network Domain seed. The Network Domain seed contains a database of all the VLANs configured on all the members of the Network Domain.
3. The Network Domain seed checks the local database and finds that VLAN Red exists in the Mobility Domain at Sales Office C. The Network Domain seed then responds with the IP address of the remote MX configured with VLAN Red.
4. A VLAN tunnel is created between the MX at the Corporate Office and the MX at Sales Office C.
5. Bob establishes connectivity on the network at the corporate office and is placed in VLAN Red.

## Network Domain Seed Affinity

When there are multiple Network Domain seeds in an installation, a Network Domain member connects to the seed with the highest configured . If that seed is unavailable, the Network Domain member connects to the seed with the next-highest affinity.

**Figure 18–3** illustrates how an MX connects to a Network Domain seed based on the configured affinity for the seed.

**Figure 18–3. Configuring an MX affinity for a Network Domain seed**

In the example above, an MX in the Mobility Domain at the corporate office is configured as a member of a Network Domain with a local seed, as well as seeds at the two branch offices and the three sales offices. The MX has an affinity value of 10 (highest) for the local seed, and an affinity value of 7 for the seed at Branch Office 1. The MX has an affinity of 5 (the default) for the other seeds in the Network Domain.

In the event that the local Network Domain seed becomes unavailable, the MX then attempts to connect to the seed at Branch Office 1, the next-highest-affinity seed. Once connected to this seed, the MX then periodically attempts to connect to the local seed. When the MX is able to connect to the local seed again, the connection to the Branch Office seed is dropped.

When you configure an MX to be a member of a Network Domain, you specify the connecting seed(s). As part of this configuration, you can also specify the seed affinity for the MX.

## Configuring a Network Domain

To configure a Network Domain:

1. Designate one or more Network Domain seed MX switches. (See **Configuring Network Domain Seeds**.)
2. Specify seed members in the Network Domain. (See **"Specifying Network Domain Seed Peer Relationships" on page 18–4**.)
3. Configure MX switches to be part of the Network Domain. (See **"Configuring Network Domain Members" on page 18–4**.)

You can view the status of a Network Domain, clear members, and clear all Network Domain configuration from an MX.

## Configuring Network Domain Seeds

In a Network Domain, a member MX consults a seed MX to determine a user VLAN membership in a remote Mobility Domain.

Use the following command to set the current MX as a seed device within a specified Network Domain:

```
set network-domain mode seed domain-name net-domain-name
```

For example, the following command sets the current MX as a seed with the Network Domain :

```
MX# set network-domain mode seed domain-name California
success: change accepted.
```

If the seed in a Network Domain is also intended to be a of the Network Domain, you must enter the following command on the seed, with the specified IP address of the seed.

```
set network-domain mode member seed-ip ip-addr [affinity num]
```

For example, the following command sets the current MX as a member of a Network Domain and the MX with IP address 192.168.9.254 as the seed:

```
MX# set network-domain mode member seed-ip 192.168.9.254
success: change accepted.
```

You can configure multiple seeds in a Network Domain. When multiple Network Domain seeds are configured, a member consults the seed with the highest configured affinity.

If you are configuring multiple seeds in the same Network Domain (for example, a seed on each physical site in the Network Domain), you must establish a peer relationship among the seeds.

## Specifying Network Domain Seed Peer Relationships

When multiple MX switches are configured as seed devices in a Network Domain, they establish a peer relationship to share information about the VLANs configured on the member devices to create identical VLAN databases. Sharing information in this way provides redundancy in case one of the seed peers becomes unavailable.

Use the following command on a Network Domain seed to specify another seed as a peer:

```
set network-domain peer ip-addr
```

You enter this command on all of the seed devices in the Network Domain, specifying each seed to every other seed, so that all of the Network Domain seeds are aware of each other.

For example, the following command sets the current MX as a peer of the Network Domain seed with IP address 192.168.9.254:

```
MX# set network-domain peer 192.168.9.254
success: change accepted.
```

This command is valid on Network Domain seeds only.

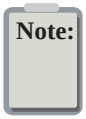
## Configuring Network Domain Members

In a Network Domain, at least one seed device must be aware of each member device. The seed maintains an active TCP connection with the member. To configure an MX as a member of a Network Domain, you specify one or more Network Domain seeds.

Use the following command to set the current MX as a member of a Network Domain where a specified MX is a seed:

```
set network-domain mode member seed-ip ip-addr [affinity num]
```

You can enter this command multiple times on an MX, specifying different Network Domain seeds with different affinity values. The affinity value can range from 1 – 10, with 10 being the highest affinity. The default affinity value is 5.




For example, the following command sets the current MX as a member of a Network Domain where the MX with IP address 192.168.9.254 is a seed:

```
MX# set network-domain mode member seed-ip 192.168.9.254
success: change accepted.
```

To specify 10.8.107.1 as an additional Network Domain seed for the MX to connect to if the 192.168.9.254 seed is unavailable, enter the following command:

```
MX# set network-domain mode member seed-ip 10.8.107.1 affinity 2
success: change accepted.
```

## Displaying Network Domain Information

To view the status of Network Domains configured on the MX, use the **show network-domain** command. The output of the command differs if the MX is a member of a Network Domain or a Network Domain seed.

For example, an MX that is a Network Domain member only, output such as the following is displayed:

```
MX# show network-domain
Member Network Domain name: California
Member              State             Mode       Mobility-Domain
---------------     -------------     ------     ---------------
10.8.107.1           P                  SEED     default
```

On an MX that is a Network Domain seed, information is displayed about the Network Domain seeds with a peer relationship to an MX, as well as the Network Domains with the MX as a member. For example:

```
MX# show network-domain
Network Domain name: California
Peer                State
---------------     -------------
10.8.107.1           P
Member              State             Mode       Mobility-Domain
---------------     -------------     ------     ---------------
10.1.0.0            DOWN                SEED
Member Network Domain name:
Member              State             Mode       Mobility-Domain
---------------     -------------     ------     ---------------
10.8.107.1           P                MEMBER     default
10.1.0.0            DOWN                SEED
```

(For more information about this command and the fields in the output, see the
)

## Clearing Network Domain Configuration from an MX

You can clear all Network Domain configuration from an MX. You may want to do this in order to change an MX from one Network Domain to another, or to remove an MX entirely from a Network Domain.

To clear the Network Domain configuration from the MX, type the following command:

```
clear network-domain
```

This command has no effect if the MX is not configured as part of a Network Domain.

## Clearing a Network Domain Seed from an MX

You can remove individual Network Domain seeds from an MX configuration. To remove a specific Network Domain seed, type the following command:

```
clear network-domain seed-ip ip-addr
```

When you enter this command, the Network Domain TCP connections between the MX and the specified Network Domain seed are closed.

## Clearing a Network Domain Peer from a Network Domain Seed

On an MX configured as a Network Domain seed, you can clear the configuration of individual Network Domain peers. To remove a specific Network Domain peer from a Network Domain seed, type the following command:

```
clear network-domain peer ip-addr
```

This command has no effect if the MX is not configured as a Network Domain seed.

## Clearing Network Domain Seed or Member Configuration from an MX Switch

You can remove the Network Domain seed or member configuration from the MX. To do this, enter the following command:

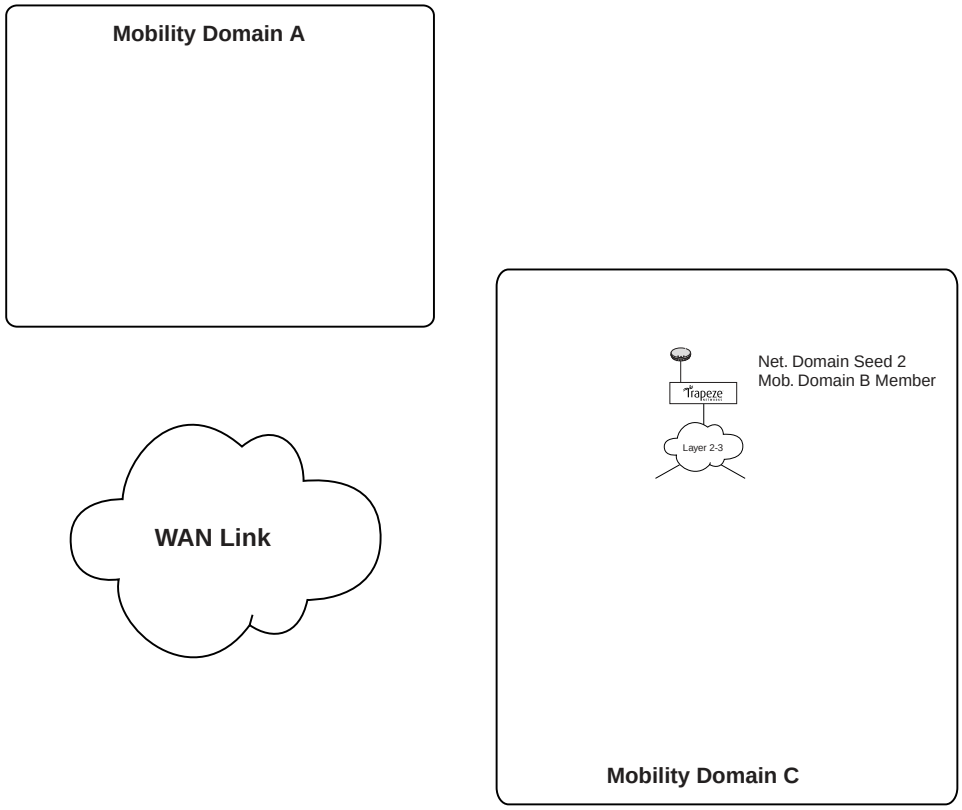
```
clear network-domain mode {seed | member}
```

Use the **seed** parameter to clear Network Domain seed configuration from the MX. Use the **member** parameter to clear Network Domain member configuration from the MX.

## Network Domain Scenario

The following scenario illustrates how to create a Network Domain named consisting of three Mobility Domains at two geographically separated sites. **Figure 18–4** below illustrates this scenario.

**Figure 18–4. Network Domain Scenario**



In this scenario, there are three Mobility Domains: A, B, and C. Mobility Domain A is located at Site 1, and Mobility Domains B and C are located at Site 2. There are two Network Domain seeds,

```
20.20.20.1          P                SEED     Modo B
20.20.20.2          P              MEMBER     Modo B
20.20.20.3          P              MEMBER     Modo B
30.30.30.1          P              MEMBER     Modo C
30.30.30.2          P              MEMBER     Modo C
```

19

# Configuring and Managing Spanning Tree Protocol

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. A loop-free path is accomplished when a

## Changing the Bridge Priority

To change the bridge priority, use the following command:

```
set spantree priority value {all | vlan vlan-id}
```

Specify a bridge priority from 0 through 65,535. The default is 32,768. The **all** option applies the change globally to all VLANs. Alternatively, specify an individual VLAN.

To change the bridge priority of VLAN to 69, type the following command:

```
MX# set spantree priority 69 vlan pink
success: change accepted.
```

## Changing STP Port Parameters

You can change the STP cost and priority of an individual port, on a global basis or an individual VLAN basis.

### Changing the STP Port Cost

To change the cost of a port, use one of the following commands.

```
set spantree portcost port-list cost cost
set spantree portvlancost port-list cost cost {all | vlan vlan-id}
```

The **set spantree portcost** command changes the cost for ports in the default VLAN (VLAN 1) only. The **set spantree portvlancost** command changes the cost for ports in a specific other VLAN or in all VLANs.

Specify a value from 1 through 65,535 for the cost. The default depends on the port speed and link type. (See Table 19– 1 on page 2.)

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

The **set spantree portpri** command changes the priority for ports in the default VLAN (VLAN 1) only. The **set spantree portvlanpri** command changes the priority for ports in a specific other VLAN or in all VLANs.

Specify a priority from 0 (highest priority) through 255 (lowest priority). The default is 128.

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

To set the priority of ports 3 and 4 in the default VLAN to 48, type the following command:

```
MX# set spantree portpri 3-4 priority 48
success: change accepted.
```

To set the priority of ports 3 and 4 to 48 in VLAN

## Changing the STP Maximum Age

To change the maximum age, use the following command:

`set spantree maxage aging-time {all | vlan` *`vlan-id`*`}`

Specify an age from 6 through 40 seconds. The default is 20 seconds.

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

## Uplink Fast Convergence

Uplink fast convergence enables an MX with redundant links to the network core to immediately change the state of a backup link to forwarding if the primary link to the root fails. Uplink fast convergence bypasses the listening and learning states to immediately enter the forwarding state.


## Configuring Port Fast Convergence

To enable or disable port fast convergence, use the following command:

```
set spantree portfast port port-list {enable | disable}
```

To enable port fast convergence on ports 9, 11, and 13, type the following command:

```
MX# set spantree portfast port 9,11,13 enable
success: change accepted.
```

## Displaying Port Fast Convergence Information

To display port fast convergence information, use the following command:

```
show spantree portfast [port-list]
```

To display port fast convergence information for all ports, type the following command:

```
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
```

In this example, port fast convergence is enabled on ports 11 and 14 in VLAN 2 and port 4 in VLAN 1.

## Configuring Backbone Fast Convergence

To enable or disable backbone fast convergence, use the following command:

```
set spantree backbonefast {enable | disable}
```

To enable backbone fast convergence on all VLANs, type the following command:

```
MX# set spantree backbonefast enable
success: change accepted.
```

### Displaying the Backbone Fast Convergence State

To display the state of the backbone fast convergence feature, use the following command:

```
show spantree backbonefast
```

Here is an example:

```
MX# show spantree backbonefast


 Backbonefast is enabled
```

In this example, backbone fast convergence is enabled.

### Configuring Uplink Fast Convergence

To enable or disable uplink fast convergence, use the following command:

```
set spantree uplinkfast {enable | disable}
```

### Displaying Uplink Fast Convergence Information

To display uplink fast convergence information, use the following command:

```
show spantree uplinkfast [vlan vlan-id]
```

The following command displays uplink fast convergence information for all VLANs:

```
MX# show spantree uplinkfast
 VLAN    port    list
------------------------------------------------------------------------
1       1(fwd),2,3
```

In this example, ports 1, 2, and 3 provide redundant links to the network core. Port 1 is forwarding traffic. The remaining ports block traffic to prevent a loop.

## Displaying Spanning Tree Information

You can use CLI commands to display the following STP information:

- Bridge STP settings and individual port information
- Blocked ports
- Statistics
- Port fast, backbone fast, and uplink fast convergence information


### Displaying STP Bridge and Port Information

To display STP bridge and port information, use the following command:

```
show spantree [port port-list | vlan vlan-id] [active]
```

By default, STP information for all ports and all VLANs is displayed. To display STP information for specific ports or a specific VLAN only, enter a port list or a VLAN name or number. For each VLAN, only the ports contained in the VLAN are listed in the command output.

To list only the ports that are in the active (forwarding) state, enter the **active** option.

To display STP information for VLAN , type the following command:

```
MX# show spantree vlan mauve
VLAN     3
Spanning tree mode           PVS +
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  ime 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  ime 2 sec   Forward Delay 15 sec

Port               Vlan       S P-State    Cost   Prio   Portfast
-------------------------------------------------------------------------------
1                   1        Forwarding      19   128     Disabled
2                   1        Blocking        19   128     Disabled
3                   1        Blocking        19   128     Disabled
10                  1        Forwarding      19   128     Disabled
15                  1        Blocking        19   128     Disabled
16                  1        Blocking        19   128     Disabled
```

In this example, VLAN contains ports 1 through 3, 10, 15 and 16. Ports 1 and 10 are forwarding traffic. The other ports are blocking traffic.

(For more information about the fields in the output, see the )

## Displaying the STP Port Cost by VLAN

To display a brief list of the STP port cost for a port in each of the VLANs, use the following command:

`show spantree portvlancost` *`port-list`*

This command displays the same information as the **show spantree** command Cost field in a concise format for all VLANs. The **show spantree** command lists all the STP information separately for each VLAN.

To display the STP port cost of port 1, type the following command:

```
MX# show spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

## Displaying Blocked STP Ports

To display information about ports that are in the STP blocking state, use the following command:

`show spantree blockedports [vlan` *`vlan-id`*`]`

To display information about blocked ports on an MX for the VLAN (VLAN 1), type the following command:

```
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
```

(For information about the fields in the output, see the .)

## Displaying Spanning Tree Statistics

To display STP statistics, use the following command:

```
show spantree statistics [port-list [vlan vlan-id]]
```

To display STP statistics for port 1, type the following command:

```
MX# show spantree statistics 1

BPD  related parameters


Port 1                    VLAN 1
spanning tree enabled for VLAN = 1
port spanning tree                          enabled
state                                       Forwarding
port_id                                     0x8015
port_number                                 0x15
path cost                                   0x4
message age (port/VLAN)                     0(20)
designated_root                             00-0b-0e-00-04-30
designated cost                             0x0
designated_bridge                           00-0b-0e-00-04-30
designated_port                             38
top_change_ack                              FALSE
config_pending                              FALSE
port_inconsistency                          none


             Port based information statistics

config BPD 's xmitted(port/VLAN)            0 (1)
config BPD 's received(port/VLAN)           21825 (43649)
tcn BPD 's xmitted(port/VLAN)               0 (0)
tcn BPD 's received(port/VLAN)              2 (2)
forward transition count (port/VLAN)        1 (1)
scp failure count                           0
root inc trans count (port/VLAN)            1 (1)
inhibit loopguard                           FALSE
loop inc trans count                        0 (0)


            Status of Port  imers

forward delay timer                         INAC IVE
forward delay timer value                   15
message age timer                           AC IVE
message age timer value                     0
topology change timer                       INAC IVE
topology change timer value                 0
hold timer                                  INAC IVE
hold timer value                            0
delay root port timer                       INAC IVE
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
```

```
last topology change occurred:            ue 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 BPD  ok count                        21825
msg age expiry count                      0
link loading                              0
BPD  in processing                        FALSE
num of similar BPD '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
```

(For information about the fields in the output, see the .)

### Clearing STP Statistics

To clear the STP statistics counters, use the following command.

`clear spantree statistics` *port-list* [vlan *vlan-id*]

As soon as you enter the command, MSS resets the STP counters for the specified ports or VLANs to 0. The software then begins incrementing the counters again.

## Spanning Tree Configuration Scenario

This scenario configures a VLAN named for connections from a MX to the network backbone, adds ports 21 and 22 to the VLAN, and enables STP on the VLAN to prevent loops.

1. Remove the network cables from ports 21 and 22 or use MSS to disable the ports,. This prevents a loop until you complete the STP configuration. To disable the ports and verify the results, type the following commands:

```
MX# set port disable 21-22
success: set "disable" on port 21-22
MX# show port status
Port  Name            Admin  Oper    Config    Actual     ype       Media
=============================================================================
   1                  up     up      auto      100/full  network    10/100Base x
   2                  up     down    auto                network    10/100Base x
   3                  up     down    auto                network    10/100Base x
   4                  up     down    auto                network    10/100Base x
   5                  up     down    auto                network    10/100Base x
   6                  up     down    auto                network    10/100Base x
   7                  up     down    auto                network    10/100Base x
   8                  up     down    auto                network    10/100Base x
   9                  up     down    auto                network    10/100Base x
  10                  up     down    auto                network    10/100Base x
  11                  up     down    auto                network    10/100Base x
  12                  up     down    auto                network    10/100Base x
  13                  up     down    auto                network    10/100Base x
  14                  up     down    auto                network    10/100Base x
  15                  up     down    auto                network    10/100Base x
```

```
  16                  up     down    auto                network    10/100Base x
  17                  up     down    auto                network    10/100Base x
  18                  up     down    auto                network    10/100Base x
  19                  up     down    auto                network    10/100Base x
  20                  up     down    auto                network    10/100Base x
  21                down     down    auto                network
  22                down     down    auto                network
```

**2.** Configure a VLAN and verify the configuration change. Type the following commands:

```
MX# set vlan 10 name backbone port 21-22
success: change accepted.
MX# show vlan config
                    Admin  VLAN   unl                          Port
VLAN Name           Status State Affin Port             ag    State
---- -------------- ------ ----- ----- -------------- ----- -----
   1 default          p      p        5
                                        1              none   p
  10 backbone         p     Down      5
                                       21              none  Down
                                       22              none  Down
```

**3.** Enable STP on the

# Configuring Quality of Service

This chapter describes the Quality of Service (QoS) features supported in MSS and how to configure and manage them.

## About QoS

Quality of Service (QoS) protocols on a network can guarantee a certain level of throughput for a specific path, connection, or type of traffic. This makes it possible to ensure that critical network applications receive priority handling.

MSS supports Layer 2 and Layer 3 classification and marking of traffic, and prioritized forwarding of wireless traffic for time-sensitive applications such as voice and video.

For more information on QoS, consult any networking protocol reference available on the Internet or in book format.

### Summary of QoS Features

QoS features are configured in radio profiles and service profiles. **Table 20– 1** lists the QoS features in MSS.

**Table 20– 1. QoS Parameters**

| QoS Feature | Description | Configuration Command |
|---|---|---|
| **QoS parameters configured in the radio profile** | | |
| QoS mode | Meth used to con tion w low para ters of fo ard queues MPs. One the following m es can be en , ❑ S traLink Voice ority ❑ W Multi dia WMM must be configured in order to accept WMM clients. | `set radio-profile qos-mode` See the following: ❑ **"End-to-End QoS" on page 20–3** ❑ **"Changing the QoS Mode" on page 20–11** See the following: |
| WMM powersave support | Unscheduled Automatic Powersave Delivery (U-APSD). U-APSD enables clients that use powersave mode to more efficiently request buffered unicast packets from MP radios. | `set radio-profile wmm-pow-ersave` See the following: ❑ **"WMM QoS in a Trapeze Network with Local Switching" on page 20–9** ❑ |

**Table 20– 1. QoS Parameters (continued)**

| QoS Feature | Description | Configuration Command |
|---|---|---|
| Using client Differentiated Services Code Point (DSCP) value | Whether the MP classifies the QoS level for IP packets from a client based on the DSCP value, instead of the 802.11 WMM user priority. | `set service-profile use-client-dscp`<br>See **"Using the Client DSCP Value to Classify QoS Level" on page 20–13**. |
| Transmit rates | Data transmission rates supported by each radio type. The following categories are specified:<br>❑ Beacon<br>❑ Multicast<br>❑ Mandatory (a client must support at least one of these rates to associate)<br>❑ Disabled<br>❑ Standard (valid rates that are not disabled and are not mandatory)<br>Defaults:<br>❑ Mandatory:<br>❑ 802.11a—6.0, 12.0, 24.0<br>❑ 802.11b—5.5, 11.0<br>❑ 802.11g—1.0, 2.0, 5.5, 11.0<br>❑ Disabled—None. All rates applicable to the radio type are supported by default.<br>❑ Beacon:<br>❑ 802.11a—6.0<br>❑ 802.11b—5.5<br>❑ 802.11g—5.5<br>❑ Multicast—auto for all radio types (highest rate that can reach all associated clients is used) | `set service-profile trans-mit-rates` |
| Broadcast control | Mechanisms to reduce overhead caused by wireless broadcast traffic or traffic from unauthenticated clients. One or more of the following can be enabled:<br>❑ Proxy ARP<br>❑ No-Broadcast<br>❑ DHCP Restrict<br>All three options are disabled by default. | `set service-profile proxy-arp`<br>`set service-profile no-broadcast`<br>`set service-profile dhcp-restrict`<br>See the following:<br>❑ **"Broadcast Control" on page 20–11**<br>❑ **"Enabling Broadcast Control" on page 20–13** |
| Session timers | Keepalives and timeouts for client sessions. The following timeout parameters can be configured:<br>❑ user idle timeout—Period a client can remain idle before being disassociated (default: 180 seconds)<br>❑ idle-client probing—keepalives sent to clients (enabled by default) | `set service-profile user-idle-timeout`<br>`set service-profile idle-client-probing` |
| Bandwidth Management | Maximum bandwidth for aggregates of access categories. | `set qos-profile` *`profile-name`* `max-bw` |

**Table 20– 2** shows how WMM priority information is mapped across the network.

**Table 20– 2. WMM Priority Mappings**

| CoS | WMM User Priority | 802.1p | IP ToS | IP Precedence | DSCP | MP Forwarding Queue |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | Best Effort |
| 1 | 1 | 1 | 0x20 | 1 | 8 | Background |
| 2 | 2 | 2 | 0x40 | 2 | 16 | Background |
| 3 | 3 | 3 | 0x60 | 3 | 24 | Best Effort |
| 4 | 4 | 4 | 0x80 | 4 | 32 | Video |
| 5 | 5 | 5 | 0xa0 | 5 | 40 | |
| 6 | 6 | 6 | 0xc0 | 6 | 48 | Voice |
| 7 | 7 | 7 | 0xe0 | 7 | 56 | |

**Table 20– 3** lists the default mappings between internal CoS values on an MP and the forwarding queues.

**Table 20– 3. CoS-to-MP-Forwarding-Queue Mappings**

| CoS | MP Forwarding Queue (Access Category) |
|---|---|
| 1 or 2 | Background |
| 0 or 3 | Best Effort |
| 4 or 5 | Video |
| 6 or 7 | Voice |

To display CoS mappings and queue usage statistics on an MP, see **"Displaying MP Forwarding Queue Statistics" on page 20–16**.

**Figure 20–1 on page 6** describes classifying ingress traffic. **Figure 20–2 on page 7** describes marking egress traffic. The figures also describe the default mappings between DSCP and CoS. (For information about changing CoS mappings, see **"Changing CoS Mappings" on page 20–13**.)

## QoS Mode

The MP has four forwarding queues, one per access category, for unicast packet traffic. The queue behavior is based on the QoS mode. The following QoS modes are supported:

- Wi-Fi Multimedia (WMM)—Provides wireless QoS for time-sensitive applications such as voice and video. WMM QoS is enabled by default and does not require any configuration.
- SpectraLink Voice Priority (SVP)—Provides optimized forwarding of SVP voice traffic. SVP QoS is disabled by default.

The SVP QoS mode optimizes the forwarding of SVP traffic for voice by setting the contention window on an MP radio to 0 microseconds.

Normally, an MP radio waits an additional number of microseconds following the fixed wait time, before forwarding a queued packet or frame. Each forwarding queue has a different range of possible random wait times. The Voice queue has the narrowest range, whereas the Background and Best Effort queues have the widest range. The random wait times ensure that the Voice queue gets statistically more access to the air than the other queues.

By setting the random wait time to 0 for SVP, the SVP QoS mode provides SVP traffic the greatest possible access to the air, on a statistical basis. The QoS mode affects forwarding of SVP traffic only. The random wait times for other types of traffic are the same as those used when the QoS mode is WMM.

## Static CoS

You can configure MSS to mark all wireless traffic on an SSID with a specific CoS value. When static CoS is enabled, the MP marks all traffic between clients and the MX for a given SSID with the static CoS value. The static CoS value must be configured on the SSID service profile.

Static CoS has the easiest configuration of CoS. However, the static CoS value applies to all traffic regardless of traffic type. To instead assign CoS based on specific traffic types within an SSID, use an ACL.


## CoS ACLs

You can configure an ACL that marks packets matching the ACL with a CoS value. CoS is not changed in packets that do not match the ACL rule.

In local switching mode, ACLs affect the packet flow within the MP. For more information, see **“Using ACLs to Change CoS” on page 24–15**.

**Figure 20–1. QoS—Classification of Ingress Packets**

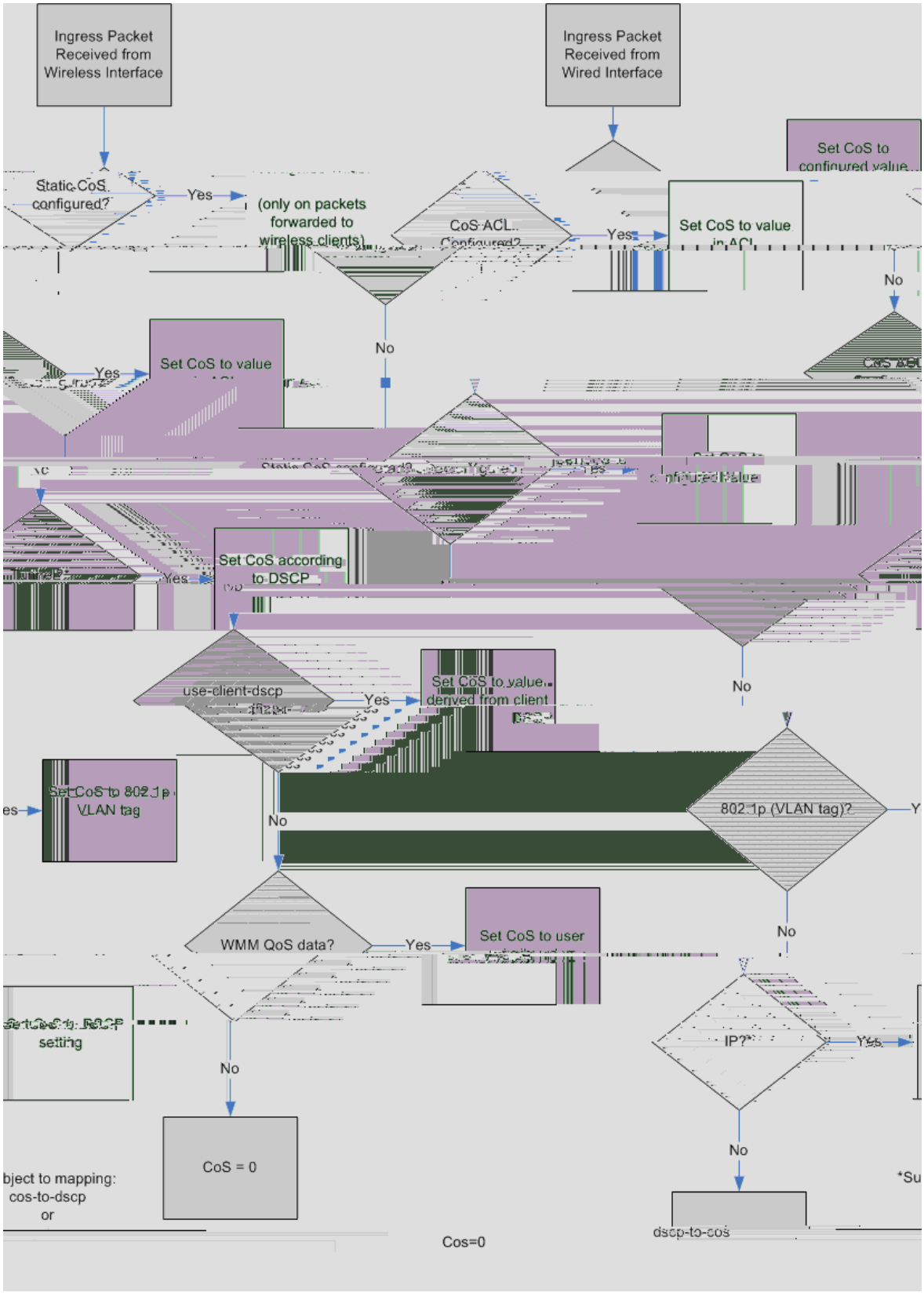


**Figure 20–2. QoS—Marking of Egress Packets**

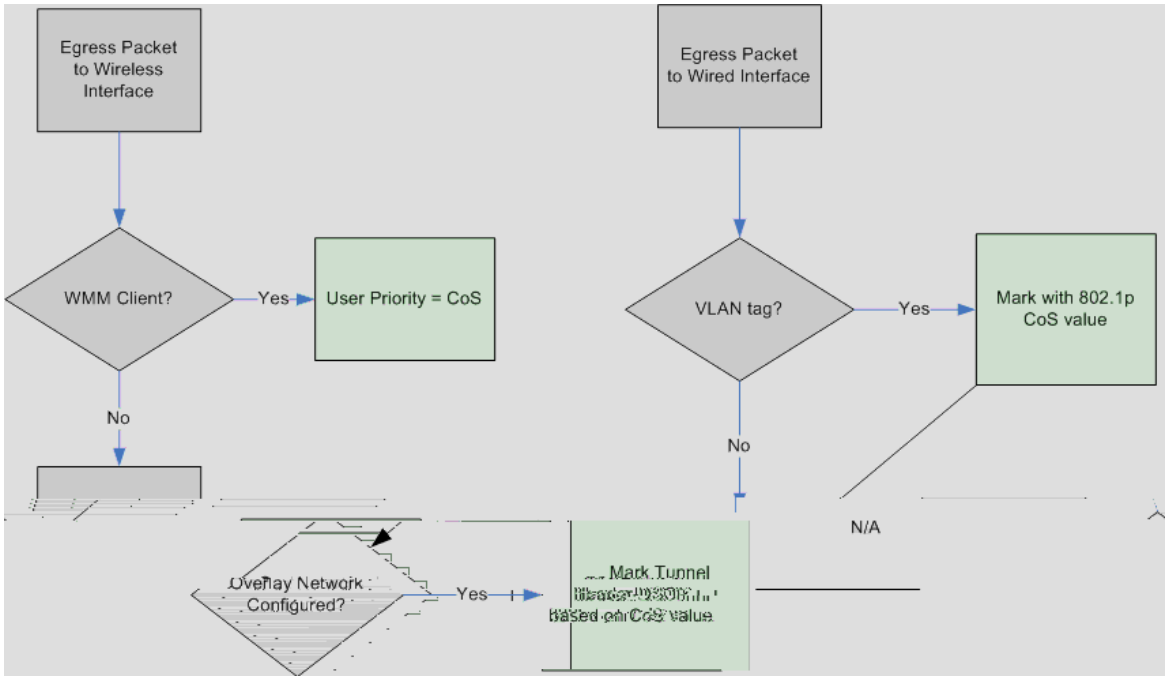



**Figure 20–3** shows an example of end-to-end QoS in a Trapeze network. In this example, voice traffic is prioritized based on WMM. This example assumes that the QoS mappings are set to the default values.

**Figure 20–3. WMM QoS in a Trapeze Overlay Network**

**Figure 20–3** shows the following process:

1. A user sends voice traffic from a WMM VoIP phone. The phone marks the CoS field of the packet with user priority 7, indicating that the packet is for high priority (voice) traffic.
2. MP A receives the voice packet and classifies the packet by mapping the user priority in the 802.11 header to an internal CoS value. In this example, the user priority is 7 and maps to internal CoS 7.

   The MP encapsulates the data in an IP tunnel packet, and marks the DSCP value in the tunnel header based on the internal CoS value. In this example, the MP maps internal CoS 7 to DSCP 56 and marks the IP tunnel header DSCP field with value 56. The MP then sends the packet to the MX switch.
3. MX A receives the packet on the IP tunnel connecting the MX to MP A. The MX classifies the packet based on the DSCP value in the IP header of the tunnel packet (in this example, DSCP

**Figure 20–4. WMM QoS in a Trapeze Network with Local Switching**

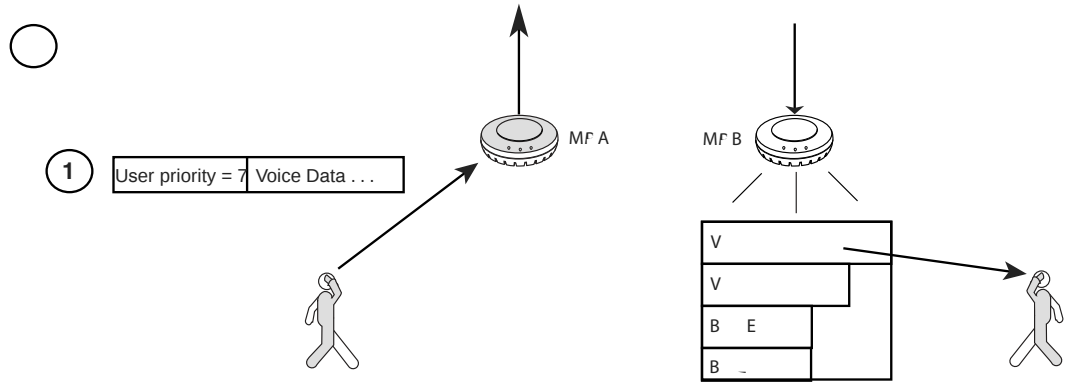



**Figure 20–4** shows the following process:

1. A user sends voice traffic from a WMM VoIP phone. The phone marks the CoS field of the packet with user priority 7, indicating that the packet is for high priority (voice) traffic.
2. MP A receives the voice packet and classifies the packet by mapping the user priority in the 802.11 header to an internal CoS value.
3. The MP marks the 802.1p value as 7 based on the internal CoS value (7), and then uses the internal CoS value to set the 802.1p value in the VLAN tag.
4. The MP sends the data in an IP packet to the Layer 3 network.
5. Because the network is configured for local switching, the packet is then sent directly to MP B.
6. MP B receives the packet and does the following:

- Classifies the packet using 802.1p tag to mark an internal CoS value (7).
- Marks the packet user priority based on the internal CoS value (7).
- Places the packet in a forwarding queue (Voice) based on the internal CoS value (7).

In this example, the MP places the packet in the Voice forwarding queue. The Voice queue has statistically more access to the air than the other queues, so voice traffic receives priority treatment.

## Bandwidth Management for QoS

You can configure maximum bandwidth (full duplex rate) for aggregates of access categories (ACs) for a wireless client. Downstream packets are shaped and upstream packets are policed. The MP has one queue per AC and each queue is a finite size (<100 packets). If the network to MP flow exceeds the determined rate, the MP queue overflows and packets are sent to the MP radio AC queues independently. The VoIP queue is given more transmit opportunities and therefore empties faster than other queues. To configure this feature, use the following command:

```
MX# set qos-profile profile-name max-bw max-bw-kb
```

The attribute is a value between 1 and 100,000 Kbps.

If you configure SSID medium time weights, you are guaranteeing a minimum service level to specific service profiles on a radio. Medium time weights determine the relative transmit utilization of the radio between service profiles. You can configure the weight from 1 to 100 with 100 as the sum of all configured weights.

To configure SSID medium weights, use the following command:

```
MX# set radio-profile profile-name
```

## Session Timers

For example, the following command enables U-APSD on radio profile :

```
MX# set radio-profile rp1 qos-mode svp
success: change accepted.
```

## Configuring Call Admission Control

To configure CAC for an SSID, enable the feature on the SSID service profile. When enabled, CAC limits the number of active sessions to 14 on a radio by default. You can change the maximum number of sessions to a value from 0 to 100.

### Enabling CAC

To enable or disable CAC on a service profile, use the following command:

```
set service-profile profile-name cac-mode {none | session}
```

For example, to enable session-based CAC on service profile , use the following command:

```
MX# set service-profile sp1 cac-mode session
success: change accepted.
```

### Changing the Maximum Number of Active Sessions

When CAC is enabled, the maximum number of active sessions a radio can have is 14 by default. To change the maximum number of sessions, use the following command:

```
set service-profile profile-name cac-session max-sessions
```

The can be a value from 0 to 500.

For example, to change the maximum number of sessions for radios used by service profile to 10, use the following command:

```
MX# set service-profile sp1 cac-session 10
success: change accepted.
```

## Configuring Session Timers

To configure session timers, you must set the idle-client-probing parameter of the service profile configuration. Use the following commands to set the session timers:

```
set service-profile profile-name idle-client-probing {enable|disable}
set service-profile profile-name {use-client-dscp|user-idle-timeout}
set service profile profile-name user-idle-timeout timeout
 he timeout value is an integer between 20 and 86400 seconds.  he default value is
        180 seconds.
```

For example, to configure session timeout for service profile use the following commands:

```
MX# set service-profile sp1 idle-client-probing enable
success: change accepted.
MX# set service-profile sp1 user-idle-timeout 180
success: change accepted.
```

## Configuring Static CoS

To configure static CoS for an SSID, enable the feature and set the CoS value. MP radios that forward traffic for the SSID mark all the traffic with the static CoS value and use the corresponding forwarding queue to forward the traffic. The static CoS value applies to all traffic on the SSID.

To enable static CoS and set the CoS value, use the following commands:

```
set service-profile profile-name static-cos {enable | disable}
set service-profile profile-name cos level
```

The can be a value from 0 (lowest priority) to 7 (highest priority). The default is 0.

For example, to configure static CoS 7 for service profile , use the following commands:

```
MX# set service-profile sp1 static-cos enable
success: change accepted.
```

```
MX# set service-profile sp1 cos 7
success: change accepted.
```

## Changing CoS Mappings

To change CoS mappings, use the following commands:

```
set qos dscp-to-cos-map dscp-range cos level
set qos cos-to-dscp-map level dscp dscp-value
```

The first command changes the mapping of ingress DSCP values to the internal QoS table when marking packets. The second command changes the mappings of the internal QoS values to DSCP value when tagging outbound packets.

The following command changes the mapping of DSCP value 45 from CoS value 5 to CoS value 7. The change affects classification but does not affect marking.

```
MX# set qos dscp-to-cos-map 45 cos 7
success: change accepted.
```

The following command changes the mapping of CoS value 6 from DSCP value 48 to DSCP value 55. The change affects marking but does not affect classification.

```
MX# set qos cos-to-dscp-map 6 dscp 55
success: change accepted.
```

## Using the Client DSCP Value to Classify QoS Level

To configure MSS to classify the QoS level of IP packets based on their DSCP value, instead of 802.11 priority, use the following command:

```
set service-profile profile-name use-client-dscp {enable | disable}
```

If this command is enabled in the service profile, the 802.11 QoS level is ignored, and MSS classifies QoS level of IP packets based on a DSCP value.

The following command enables mapping the QoS level of IP packets based on a DSCP value for service profile :

```
MX# set service-profile sp1 use-client-dscp enable
success: change accepted.
```

## Enabling Broadcast Control

To enable broadcast control features on a service-profile basis, using the following commands:

```
set service-profile profile-name
```

- The DSCP table (a reference of standard mappings from DSCP to IP ToS and IP precedence)
- QoS Statistics for the MP forwarding queues

## Displaying QoS Settings for a Radio Profile

To display the QoS mode and all other settings for a radio profile, use the following command:

```
show radio-profile {profile-name | ?}
```

The following example shows the configuration of radio profile .

```
MX# show radio-profile rp1
Beacon Interval:                100   D IM Interval:                    1
Max  x Lifetime:               2000   Max Rx Lifetime:               2000
R S  hreshold:                 2346   Frag  hreshold:                2346
Long Preamble:                   no    une Channel:                    yes
 une Power:                      no    une Channel Interval:          3600
 une Power Interval:            600   Power ramp interval:             60
Channel Holddown:               300   Countermeasures:               none
Active-Scan:                    yes   RFID enabled:                    no
WMM Powersave:                   no   QoS Mode:                       wmm

Service profiles: sp1
```

In this example, the QoS mode is WMM and U-APSD support (WMM powersave) is disabled.

(For more information about the command output, see the “MP Access Point Commands” chapter in the )

## Displaying QoS Settings for a Service Profile

To display QoS settings and all other settings for a service profile, use the following command:

```
show service-profile {profile-name | ?}
 he following example shows the configuration of the sp1 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
CAC mode:                     session   CAC sessions:                    14
 ser idle timeout:                180   Idle client probing:            yes
Keep initial vlan:                 no   Web Portal Session  imeout:       5
Web Portal ACL:
WEP Key 1 value:               <none>   WEP Key 2 value:             <none>
WEP Key 3 value:               <none>   WEP Key 4 value:             <none>
WEP  nicast Index:                  1   WEP Multicast Index:              1
Shared Key Auth:                   NO
WPA enabled:
    ciphers: cipher-tkip
    authentication: 802.1X
     KIP countermeasures time: 60000ms
11a beacon rate:                 6.0   multicast rate:                 A  O
```

### Displaying CAC Session Information

To display current CAC session counts on all MPs using a specified service profile, when session-based CAC is enabled, use the following command:

```
show service-profile profile-name cac session
```

The following example displays information about CAC session counts for service profile :

```
MX# show service-profile sp1 cac session
Service Profile   sp1
CAC Mode          SESSION
Max Sessions      14
```

## Displaying CoS Mappings

MSS provides commands for displaying the default CoS mappings and configured mappings.

### Displaying the Default CoS Mappings

To display the default CoS mappings, use the following command:

```
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  oS byte      0x00   0x20   0x40   0x60   0x80   0xA0   0xC0   0xE0
```

### Displaying a DSCP-to-CoS Mapping

To display the CoS value to which a specific DSCP value is mapped during classification, use the following command:

```
show qos dscp-to-cos-map dscp-value
```

The following command displays the CoS value to which DSCP value 55 is mapped:

```
MX# show qos dscp-to-cos-map 55
dscp 55 is classified as cos 6
```

### Displaying a CoS-to-DSCP Mapping

To display the DSCP value to which a specific CoS value is mapped during marking, use the following command:

```
show qos cos-to-dscp-map cos-value
```

The following command displays the DSCP value to which CoS value 6 is mapped:

```
MX# show qos cos-to-dscp-map 6
cos 6 is marked with dscp 48 (tos 0xC0)
```

```
Queue              x Packets         x Dropped       Re- ransmit
Background                 0                 0                 0
BestEffort               647                 0                89
Video                      0                 0                 0
Voice                      0                 0                 0
```

The last table displays QoS packets sorted by background, best effort, video, and voice. This information is useful when attempting to troubleshoot your QoS configuration.

# Configuring and Managing IGMP Snooping

Internet Group Management Protocol (IGMP) snooping controls multicast traffic on an MX by forwarding packets for a multicast group only on the ports that are connected to members of the group. A multicast group is a set of IP hosts that receive traffic addressed to a specific Class D IP address, the group address.

The MX listens for mt

# Changing IGMP Timers

You can change the following IGMP timers:

- Query interval—Number of seconds that elapse between general queries sent by the MX to advertise multicast groups.
- Other-querier-present interval—Number of seconds that the MX waits for a general query to arrive from another querier before becoming the querier.
- Query response interval—Number of seconds, in tenths, that the MX waits for a receiver to respond to a group-specific quer

### Changing Robustness

Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network. Set the robustness value higher to adjust for more traffic loss. To change the robustness value, use the following command:

```
set igmp rv num [vlan vlan-id]
```

You can specify a value from 2 through 255. The default is 2.

## Enabling Router Solicitation

An MX can search for multicast routers by sending multicast router solicitation messages. This message invites multicast routers receiving the message and support router solicitation to immediately advertise themselves to the MX. Router solicitation is disabled by default.

The MSS implementation of router solicitation is based on .

To enable or disable multicast router solicitation, use the following command:

```
set igmp mrsol {enable | disable} [vlan vlan-id]
```

### Changing the Router Solicitation Interval

The default multicast router solicitation interval is 30 seconds. To change the interval, use the following command:

```
set igmp mrsol mrsi seconds [vlan vlan-id]
```

You can specify 1 through 65,535 seconds. The default is 30 seconds.

## Configuring Static Multicast Ports

An MX learns about multicast routers and receivers from multicast traffic it receives from those devices. When the MX receives traffic from a multicast router or receiver, the switch adds the port that received the traffic as a multicast router or receiver port. The MX forw

# Displaying Multicast Information

You can use the CLI to display the following IGMP snooping information:

- Multicast configuration information and statistics
- Multicast queriers
- Multicast routers
- Multicast receivers

## Displaying Multicast Configuration Information and Statistics

To display multicast configuration information and statistics, use the following command:

`show igmp [vlan vlan-id]`

The **show igmp** command displays the IGMP snooping state, the settings of all multicast parameters you can configure, and multicast statistics.

To display multicast information for VLAN , type the following command:

```
MX# show igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast
router information:
Port Mrouter-IPaddr Mrouter-MAC         ype    L
---- -------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    17
Group           Port Receiver-IP     Receiver-MAC        L
--------------- ---- --------------- ----------------- -----
      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         L
---- --------------- ----------------- -----
   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  ransmitted 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- erm             0           0       0
Mrouter-Sol             50         101       0
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
 opology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad chatic
Packets with unknown IGMP type: 0
```

Use the **group** parameter to display receivers for a specific group or set of groups. For example, to display receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs, type the following command:

```
MX# show igmp receiver-table group 237.255.255.0/24
VLAN: red
Session         Port Receiver-IP     Receiver-MAC        L
--------------- ---- --------------- ----------------- -----
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        L
--------------- ---- --------------- ----------------- -----
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
```

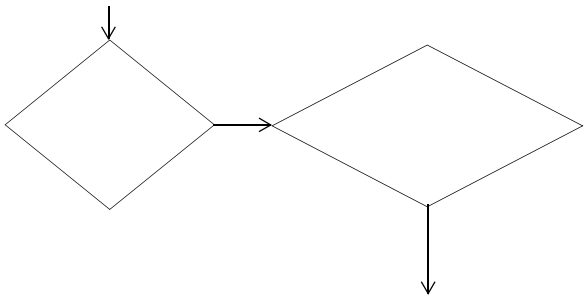
(For information about the fields in the output, see the .)

22

# Rogue Detection and Countermeasures

MP radios automatically scan the RF spectrum for other devi

**Figure 22–1. Rogue Detection Algorithm**



## RF Detection Scans

All radios continually scan for other RF transmitters. Radios perform passive and active scans:

- Passive scans—The radio listens for beacons and probe responses.
- Active scans—The radio sends requests (probe requests with a null SSID name) to solicit probe responses from other access points.

Passive scans are always enabled and cannot be disabled. Active scans are enabled by default but can be disabled on a radio-profile basis.

Radios perform both types of scans on all channels allowed for the country of operation. (This is the regulatory domain set by the **set system countrycode** command.) 802.11b/g radios scan in the 2.4 GHz to 2.4835 GHz spectrum. 802.11a radios scan in the 5.15 GHz to 5.85 GHz spectrum.

The active-scan algorithm is sensitive to high-priority (voice or video) traffic or heavy data traffic. Active-scan scans for 30 msec once every second, unless either of the following conditions is true:

- High-priority traffic (voice or video) is present at 64 Kbps or higher. In this case, active-scan scans for 30 msec every 60 seconds.
- Heavy data traffic is present at 4 Mbps or higher. In this case, active-scan scans for 30 msec every 5 seconds.

If you select passive mode, the radio scans once per predefined time, and audits packets on the wireless network. The default time is one second.

If you select active mode, the radio actively sends probes to other channels and then audits the packets on the wireless network.

To configure the channel scope for RF scanning, use the following command:

```
MXR-2# set radio-profile profile-name rf-scanning channel-scope operating|regula-
       tory|all]
```

When you select the attribute, , only the current channel is scanned and audited. If you select regulatory, only regulatory channels are scanned and audited. If the radio is configured for 802.11b/g, the most commonly used channels, such as 1, 6, or 11, are scanned and audited more frequently. Selecting all means that all channels are scanned and audited.

Radio configuration now has the capability of separate scanning behaviors independently controlled by separate attributes. For example, a “disabled” radio does not transmit or receive, and a radio that is scanning but not providing radio service to clients is in “sentry” mode.

In addition, there is an enhanced capability to weight scanning time on the radios. By weighting the scanning time, a higher proportion of time is spent on “operational” channels. This enhancement increases the probability that an event of interest is detected within a short time.

The MP LED behavior has changed to support this feature. If the MP is in sentry mode, the LEDs alternate between green and yellow/amber. If the radio is disabled, the LED is a solid yellow/amber color.

## Dynamic Frequency Selection (DFS)

Some regulatory domains require

### Countermeasures

You can enable MSS to use countermeasures against rogues. Countermeasures consist of packets that interfere with the ability of a client to use the rogue.

Countermeasures are disabled by default. You can enable them on an individual radio-profile basis. When you enable them, all devices of interest not in the known devices list become viable targets for countermeasures. Countermeasures can be enabled against all rogue and interfering devices, against rogue devices only, or against devices explicitly configured in the MX attack list. The Mobility Domain seed switch automatically selects individual radios to send the countermeasure packets.

### Mobility Domain Requirement

RF Detection requires the Mobility Domain to be completely up. If a Mobility Domain is not fully operational (not all members are up), no new RF Detection data is processed. Existing RF Detection information ages out normally. Processing of RF Detection data is resumed only when all members of the Mobility Domain are up. If a seed MX in the Mobility Domain cannot resume full operation, you can restore the Mobility Domain to full operation, and therefore resume RF Detection data processing, by removing the inoperative switch from the member list on the seed.

## Summary of Rogue Detection Features

**Table 22– 1** lists the rogue detection features in MSS.

**Table 22– 1. Rogue Detection Features**

# Configuring Rogue Detection Lists

The following sections describe how to configure lists to specify the devices that are allowed on the network and the devices that MSS should attack with countermeasures.

(For information about how MSS uses the lists, see **"Rogue Detection Lists" on page 22–2**.)

## Configuring a Permitted SSID List

The permitted SSID list specifies the SSIDs allowed on the network. If MSS detects packets for an SSID not on the list, the AP sending the packets is classified as a rogue. MSS issues countermeasures against the rogue if they are enabled.

By default, the permitted SSID list is empty and all SSIDs are allowed. If you configure a permitted SSID list, MSS allows traffic only for the SSIDs on the list. The permitted SSID list applies only to the configured list on the MX. MX switches do not share permitted SSID lists.

If you add a device that MSS has classified as a rogue to the SSID list, but not to the ignore list,

## Configuring a Client Blacklist

The Client Blacklist specifies clients not allowed

To display the Rogue list, use the following command:

```
show rfdetect attack-list
```

The following example shows the Rogue list on a MX:

```
MX# show rfdetect rogue-list
 otal number of entries: 1
 Attacklist MAC    Port/Radio/Chan   RSSI      SSID
----------------- ----------------- ------ ------------
11:22:33:44:55:66   ap 2/1/11       -53    rogue-ssid
```

To remove a MAC address from the attack list, use the following command:

```
clear rfdetect rogue-list mac-addr
```

The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
MX# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

## Configuring an Neighbor List

By default, when countermeasures are enabled, MSS considers any non-Trapeze transmitter to be a rogue device and can send countermeasures to prevent clients from using that device. To prevent MSS from sending countermeasures against a friendly device, add the device to the known devices list:

# Enabling Countermeasures

Countermeasures are disabled by default. You can enable them on an individual radio profile basis. To enable countermeasures on a radio profile, use the following command:

```
set radio-profile profile-name countermeasures {all | rogue | none}
```

The **all** option enables or disables countermeasures 42k rogues and 42k interfering devices. This option is equivalent to the scope of rogue detection in MSS Version 3.x. The **rogue** option enables or disables countermeasures 42k rogues only.

The **none** option disables countermeasures 42k this radio profile.

The following command enables countermeasures in radio profile 42k rogues only:

```
MX# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The 42llowing command causes radios managed by radio profile to issue countermeasures against devices in the MX attack list:

```
MX# set radio-profile radprof3 countermeasures configured
success: change accepted.
```

# IDS and DoS Alerts

MSS can detect illegitimate network access attempts and attempts to disrupt network service. In response, MSS generates messages and SNMP notifications. The following sections describe the types of attacks and security risks that MSS can detect.

For examples of the log messages that MSS generates when DoS attacks or other security risks are detected, see "IDS Log Message Examples" on page 12.

For information about the notifications, see **"Configuring a Notification Profile" on page 9–5**.


## Flood Attacks

A flood attack is a type of Denial of Service attack. During a flood attack, a rogue wireless device attempts to overwhelm the resources of other wireless devices by continuously injecting management frames into the air. For example, a rogue client can repeatedly send association requests to try and overwhelm APs with requests.

The threshold for triggering a flood message is 100 frames of the same type from the same MAC address, within a one-second period. If MSS detects more than 100 of the same type of wireless frame within one second, MSS generates a log message. The message indicates the frame type, the MAC address of the sender, the listener (MP and radio), channel number, and RSSI.

## DoS Attacks

When active scan is enabled on MPs, MSS can detect the following types of DoS attacks:

- RF Jamming—The goal of an RF jamming attack is to take down an entire WLAN by overwhelming the radio environment with high-power noise. A symptom of an RF jamming attack is excessive interference. If an MP radio detects excessive interference on a channel, and RF Auto-Tuning is enabled, MSS changes the radio to a different channel.
- Deauthenticate frames—Spoofed deauthenticate frames form the basis for most DoS attacks, and are the basis for other types of attacks including man-in-the-middle attacks. The source MAC address is spoofed so that clients think the packet is coming from a legitimate AP. If an MP detects a packet with the source MAC address, the MP detects that the packet was spoofed.
- Broadcast deauthenticate frames—Similar to the spoofed deauthenticate frame attack, a broadcast deauthenticate frame attack generates spoofed deauthenticate frames, with a broadcast destination address instead of the specific client address. The intent of the attack is to disconnect all stations attached to an AP.
- Disassociation frames—A disassociation frame from an AP instructs the client to end an association with the AP. The intent of this attack is to disconnect clients from the AP.
- Null probe responses—A client probe request frame is answered by a probe response containing a null SSID. Some NIC cards lock up upon receiving such a probe response.
- Decrypt errors—An excessive number of decrypt errors can indicate that multiple clients are using the same MAC address. A device's MAC address is supposed to be unique. Multiple instances of the same address can indicate that a rogue device is pretending to be a legitimate device by spoofing the MAC address.
- Fake AP—A rogue device sends beacon frames for randomly generated SSIDs or BSSIDs. This type of attack can cause clients to become confused by the presence of so many SSIDs and BSSIDs, and thus interferes with the client ability to connect to valid APs. This type of attack can also interfere with RF Auto-Tuning when an MP is trying to adjust to the RF neighborhood.
- SSID masquerade—A rogue device pretends to be a legitimate AP by sending beacon frames for a valid SSID serviced by APs in your network. Data from clients that associate with the rogue device can be accessed by the hacker controlling the rogue device.

- Spoofed AP—A rogue device pretends to be a Trapeze MP by sending packets with the source MAC address of the Trapeze MP. Data from clients that associate with the rogue device can be accessed by the hacker controlling the rogue device.

## Netstumbler and Wellenreiter Applications

Netstumbler and Wellenreiter are widely available applications that hackers can use to gather information about the APs in your network, including location, manufacturer, and encryption settings.

## Wireless Bridge

A wireless bridge can extend a wireless network outside the desired area. For example, someone can place a wireless bridge near an exterior wall to extend wireless coverage out into the parking lot, where a hacker could then gain access to the network.

## Ad-Hoc Network

An ad-hoc network is established directly among wireless clients and does not use the infrastructure network (a network using an AP). An ad-hoc network might not be an intentionally malicious attack on the network, but this type of network steals bandwidth from your infrastructure users.

## Weak WEP Key Used by Client

A weak initialization vector (IV) makes a WEP key easier to hack. MSS alerts you regarding clients who are using weak WEP IVs so that you can strengthen the encryption on these clients or replace the clients.

## Displaying Statistics Counters

To display IDS and DoS statistics counters, use the **show rfdetect counters** commands. (See “Displaying Statistics Counters” on page 12.)

**Table 22– 2. IDS and DoS Log Messages (continued)**

| Message Type | Example Log Message |
|---|---|
| Management frame E flood | Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame E message flood.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Management frame F flood | Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame F message flood.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Associate request flood | Client aa:bb:cc:dd:ee:ff is sending associate request flood on port 2 |
| Reassociate request flood | Client aa:bb:cc:dd:ee:ff is sending re-associate request flood on port 2 |
| Disassociate request flood | Client aa:bb:cc:dd:ee:ff is sending disassociate request flood on port 2 |
| Weak WEP initialization vector (IV) | Client aa:bb:cc:dd:ee:ff is using weak wep initialization vector.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Decrypt errors | Client aa:bb:cc:dd:ee:ff is sending packets with decrypt errors.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Spoofed deauthentication frames | Deauthentication frame from AP aa:bb:cc:dd:ee:ff is being spoofed.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Spoofed disassociation frames | Disassociation frame from AP aa:bb:cc:dd:ee:ff is being spoofed.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Null probe responses | AP aa:bb:cc:dd:ee:ff is sending null probe responses.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Broadcast deauthentications | AP aa:bb:cc:dd:ee:ff is sending broadcast deauthentications.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53. |
| Fake AP SSID (when source MAC address is known) | FakeAP SSID attack detected from aa:bb:cc:dd:ee:ff.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid. |
| Fake AP BSSID (when source MAC address is not known) | FakeAP BSSID attack detected.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid. |
| Spoofed SSID | AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is masquerading our ssid used by aa:bb:cc:dd:ee:fd.<br>Detected by listener aa:bb:cc:dd:ee:fc(port 2, radio 1), channel 11 with RSSI -53. |
| Wireless bridge detected | Wireless bridge detected with address aa:bb:cc:dd:ee:ff.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid. |
| Netstumbler detected | Netstumbler detected from aa:bb:cc:dd:ee:ff.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid. |
| Wellenreiter detected | Wellenreiter detected from aa:bb:cc:dd:ee:ff.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid. |
| Ad-hoc client frame detected | Adhoc client frame detected from aa:bb:cc:dd:ee:ff.<br>Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid. |
| Spoofed AP | AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is being spoofed. Received fingerprint 1122343 does not match our fingerprint 123344.<br>Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53. |
| Disallowed SSID detected | AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is not part of ssid-list.<br>Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53. |
| AP from disallowed vendor detected | AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is not part of vendor-list.<br>Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53. |

| | |
|---|---|
| Client from disallowed vendor detected | Client Mac aa:bb:cc:dd:ee:ff is not part of vendor-list. Detected by listener aa:bb:cc:dd:ee:fd(port |

## Displaying RF Detection Information

You can use the CLI commands listed in **Table 22– 3** to display rogue detection information.

(For information about the fields in the output, see the .)

## Displaying Rogue Clients

To display the wireless clients detected by an MX, use the following command:

`show rfdetect clients [mac mac-addr]`

The following command shows information about all wireless clients detected by MPs associated

```
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
```

## Displaying SSID or BSSID Information for a Mobility Domain

To display SSID or BSSID information for an entire Mobility Domain, use the following command on the seed MX:

`show rfdetect mobility-domain [ssid` *`ssid-name`* `| bssid` *`mac-addr`*`]`

The following command displays summary information for all SSIDs and BSSIDs detected in the Mobility Domain:

```
MX# show rfdetect mobility-domain
 otal number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t =  KIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor        ype  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 lines in this display are compiled from data from multiple listeners (MP radios). If an entry has the value , not all listeners agree on the value for that item. Generally, an

```
  RSSI: -85 SSID: trpz-webaaa

BSSID: 00:0b:0e:00:7a:8a Vendor:  rapeze SSID: trpz-webaaa
 ype: intfr Adhoc: no Crypto-types: clear

  MX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/1 Mac: 00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -75 SSID: trpz-webaaa

  MX-IPaddress: 10.3.8.103 Port/Radio/Ch: ap 1/1/1 Mac: 00:0b:0e:76:56:82
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -76 SSID: trpz-webaaa
```

Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (MP radios) that detected the SSID. Each set of indented lines is a separate MP listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information are shown for each of the BSSIDs, and information about the listeners for each BSSID is shown.

```
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t =  KIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
 ransmit MAC      Vendor   ype  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
...
```

## Displaying Countermeasures Information

To display the current status of countermeasures against rogues in the Mount16measurr[(agaic*( SoftwaDom.3()

# Configuring RF Auto-Tuning and Load Balancing

## RF Auto-Tuning Overview

The RF Auto-Tuning feature dynamically assigns channel and power settings to MP radios, and adjusts those settings when needed. RF Auto-Tuning can perform the following tasks:

- Assign initial channel and power settings when an MP radio is started.
- Periodically assess the RF environment and change the channel or power settings if needed.

By default, RF Auto-Tuning is enabled for channel configuration and disabled for power configuration.

## Initial Channel and Power Assignment

The following process is used to assign the channel and power to an MP radio when first enabled:

- If RF Auto-Tuning is for both channel and power assignment, the radio uses the channel and power settings in the radio profile that manages the radio. After this, the channel and power do not change unless you change the settings in the radio profile, or enable RF Auto-Tuning.
- If RF Auto-Tuning is for channel and power assignment, the radio performs an RF scan and reports the results to the MX switch managing the radio on the MP. The scan results include third-party access points. Based on the scan results, MSS sets the channel and power on the radio. MSS always selects channel and power settings that are valid for the country of operation.
- Initial channel assignment—MSS selects a channel at random from the set of valid channels for the radio type and country code. After this, each subsequent time the radio or RF Auto-TunindioTw[(cod, )-6(of36.i)4.1i

## Channel and Power Tuning

RF Auto-Tuning can change the channel or power of a radio, to compensate for RF changes such as interference, or to maintain at least the minimum data transmit rate for associated clients. A radio continues to scan on an active data channel and on other channels and reports the results to the MX.

Periodically, the MX examines these results to determine whether the channel or the power needs to be changed.

### Power Tuning

By default, the MX evaluates the scan results for possible power changes every 300 seconds (5 minutes), and raises or lowers the power level if needed.

If RF Auto-Tuning determines that a power change is needed on a radio, MSS turns the power up or down until the new power level is reached. Ramp-up or ramp-down of the power occurs in 1 dBm increments, at regular time intervals. The default interval is 60 seconds and is configurable. The power ramp amount (1 dBm per interval) is not configurable.

### Channel Tuning

By default, the MX evaluates the scan results for possible channel changes every 3600 seconds (1 hour). MSS uses the following parameters to determine whether to change the channel on a radio:

- Presence of active sessions.

  By default, if the radio has active sessions, MSS does not change the channel. If the radio does not have any active sessions, MSS uses the remaining parameters to determine whether to change the channel.

- Received signal strength indication (RSSI)
- Amount of noise on the channel
- Packet retransmission count–the rate that the radio receives retransmitted packets.
- Utilizationmdfn6(f)4.6(ao)3cuhs4(tbasedoise o6(the ))4eh1(mb power of)]1J17.1747 0 TDmu andc(dBm ive )-0
  A8(raises( t)v.4(1)Bm ive a(new )[(Peount)-6.1(A8(r.7(v.8(d. )]TJ/F1 1 Tf6

You can statically change the transmit data rates for radios, on a radio profile basis. However, RF Auto-Tuning does not change transmit rates automatically.

## RF Auto-Tuning Parameters

**Table 23– 1** lists the RF Auto-Tuning parameters and their default settings.

**Table 23– 1. Defaults for RF Auto-Tuning Parameters**

| Parameter | Default Value | Radio Behavior When Parameter Set To Default Value |
|---|---|---|
| **Radio profile parameters** | | |
| 11a-channel-range | lower bands | The lower bands are enabled by default. |
| channel-config | enable | When the radio is first enabled, RF Auto-Tuning sets the channel based on the channels in use on neighboring access points. |
| channel-interval | 3600 | Every 3600 seconds, MSS examines the RF information gathered from the network and determines whether the channel needs to be changed to compensate for RF changes. |
| channel-holddown | 900 | MSS maintains the channel setting on a radio for at least 900 seconds regardless of RF changes. |
| channel-lockdown | disable | MSS continues to dynamically change channels if needed based on network conditions. |
| ignore-clients | disable | MSS changes the channel even if clients are connected to the radio. |
| power-config | disable | MSS uses the highest power level allowed for the country of operation or the highest supported by the hardware, whichever is lower. |
| power-interval | 300 | Every 300 seconds, MSS examines the RF information gathered from the network and determines whether the power needs to be changed to compensate for RF changes. |
| power-lockdown | disabled | MSS continues to dynamically change power settings if needed based on network conditions. |
| power-ramp-interval | 60 | When RF Auto-Tuning determines that power should be increased or decreased, MSS changes the power by 1 dBm every 60 seconds until the power setting is reached. |
| **Individual radio parameters** | | |
| max-power | Maximum allowed for country of operation | RF Auto-Tuning never sets the radio power to a level that is higher than the maximum allowed for the country of operation (countrycode). |

# Changing RF Auto-Tuning Settings

## Selecting Available Channels on the 802.11a Radio

You can configure the 802.11a radio on a MP to allow certain channels to be available or unavailable. To enable this feature, use the following command:

```
set radio-profile profile-name auto-tune 11a-channel-range {lower-bands | all-bands}
```

If you select **lower bands**, MSS selects a channel from the lower eight bands in the 802.11a range of channels: 36, 40, 44, 48, 52, 56, 60, or 64. If you select **all-bands**, MSS selects a channel from the entire 802.11a range of channels: 36, 40, 44, 48, 52, 60, 64, 149, 153, 157, or 161.

## Disabling or Reenabling Channel Tuning

RF Auto-Tuning for channels is enabled by default. To disable or reenable the feature for all radios in a radio profile, use the following command:

```
set radio-profile profile-name auto-tune channel-config {enable | disable}
        [ignore-clients]
```

The **ignore-clients** option allows MSS to change the channel on a radio even if the radio has active client sessions. Without this option, MSS does not change the channel unless there are no active client sessions on the radio.

To disable channel tuning for radios in the radio profile, type the following command:

```
MX# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

## Changing the Channel Tuning Interval

The default channel tuning interval is 3600 seconds. You can change the interval to a value from 0 to 65535 seconds. 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

To enable power tuning for radios in the radio profile, type the following command:

```
MX# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

### Changing the Power Tuning Interval

The default power tuning interval is 600 seconds. You can change the interval to a value from 1 to 65535 seconds. To change the power tuning interval, use the following command:

```
set radio-profile profile-name auto-tune power-interval seconds
```

To set the power tuning interval for radios in radio profile to 240 seconds, type the following command:

```
MX# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

### Changing the Maximum Default Power Allowed On a Radio

By default, the maximum power level that RF Auto-Tuning can set on a radio is the same as the maximum power level allowed for the country of operation. To change the maximum power level that RF Auto-Tuning can assign, use the following command:

```
set ap apnum radio {1 | 2} auto-tune max-power power-level
```

The can be a value from 1 to 20.

To set the maximum power that RF Auto-Tuning can set on radio 1 on the MP access point on port 7 to 12 dBm, type the following command.

```
MX# set ap 7 radio 1 auto-tune max-power 12
success: change accepted.
```

## Locking Down Tuned Settings

You can convert dynamically assigned channels and power settings into statically configured settings, by locking them down. When you lock down channel or power settings, MSS converts the latest values set by RF Auto-Tuning into static settings.

You can lock down channel or power settings on a radio-profile basis. MSS implements the lock down by changing the **set ap radio channel** or **set ap radio tx-power** command for each radio managed by the radio profile.

To lock down channel or power settings, use the following commands:

```
set radio-profile profile-name auto-tune channel-lockdown
set radio-profile profile-name auto-tune power-lockdown
```

To verify the static settings, use the **show ap config** command.

To save the locked down settings, you must save the MX configuration.

The following commands lock down the channel and power settings for radios in radio profile :

```
MX# set radio-profile rp2 auto-tune channel-lockdown
success: change accepted.
MX# set radio-profile rp2 auto-tune power-lockdown
success: change accepted.
```

## Displaying RF Auto-Tuning Information

You can display the RF Auto-Tuning configuration, a list of RF neighbors, and the values of RF attributes.

(For information about the fields in the output, see the .)

# RF Load Balancing Overview

RF load balancing is the ability to reduce network congestion over an area by distributing client sessions across the MP access points with overlapping coverage in the area. When the total demand of nearby wireless clients exceeds the capacity of a single MP, there is no interruption of wireless services on the network.

For example, in an auditorium or lecture hall, there may be a substantial number of clients in a relatively small amount of space. While a single MP may be sufficient for providing an RF signal to the entire area, more MPs are required to deli

To assign radios to load balancing groups, use the following command:

```
set ap apnum radio radio-num load-balancing group name [rebalance]
```

Use the **rebalance** parameter to configure the radio to disassociate its client sessions and rebalance them whenever a new radio is added to the load balancing group.

To remove a radio from its specified load balancing group, use the following command:

```
clear ap apnum radio radio-num load-balancing group
```

## Specifying Band Preference for RF Load Balancing

If a client supports both the 802.11a and 802.11b/g bands, you can configure MSS to steer the client to a less-busy radio on an MP for the purpose of load balancing. A global “band-preference” option controls the degree of concealment that an MP with two radios attempts to hide one of the radios from a client with the purpose of steering the client to the other radio.

Use the following command to cause clients that support both the 802.11a and 802.11b/g radio bands to be steered to a specific radio on the MP for the purpose of load balancing:

```
set band-preference {none | 11bg | 11a}
```

## Setting Strictness for RF Load Balancing

To perform RF load balancing, MP radios with heavy client loads are less visible to new clients, and causes the new client to associate with MP radios with a lighter load.

You can specify how strictly MSS attempts to load balanced across the MP radios in the load-balancing group. When low strictness is specified (the default), heavily loaded MP radios are less visible and steer clients to less-busy MP radios, while ensuring that clients are not denied service even if all the MP radios in the group are heavily loaded.

When maximum strictness is specified, and if an MP radio has reached the maximum client load, the MP radio is invisible to new clients, and clients attempt to connect to other MP radios. In the event that all the MP radios in the group reach maximum client load, then no new clients can connect to the network.

To specify load balancing strictness across the MP radios in a load-balancing group, use the following command:

**set load-balancing strictness low med high max**

- When the **low** option is set, no clients are denied service. New clients can be steered to other MPs, but only to the extent that service can be provided to all clients. This is the default.
- When the **med** option is set, overloaded radios steer new clients to other MPs and clients attempting to connect to overloaded radios may be delayed several seconds.
- When the **high** option is set, overloaded radios steer new clients to other MPs and clients attempting to connect to MP9 0 Tw 0 -1.98 TD [(Setting Strictness for RF Load Ba148w ( )Tj /TT6 T6 1 Tf 92]TJ /T

# 24

# Configuring and Managing Security ACLs

## About Security Access Control Lists

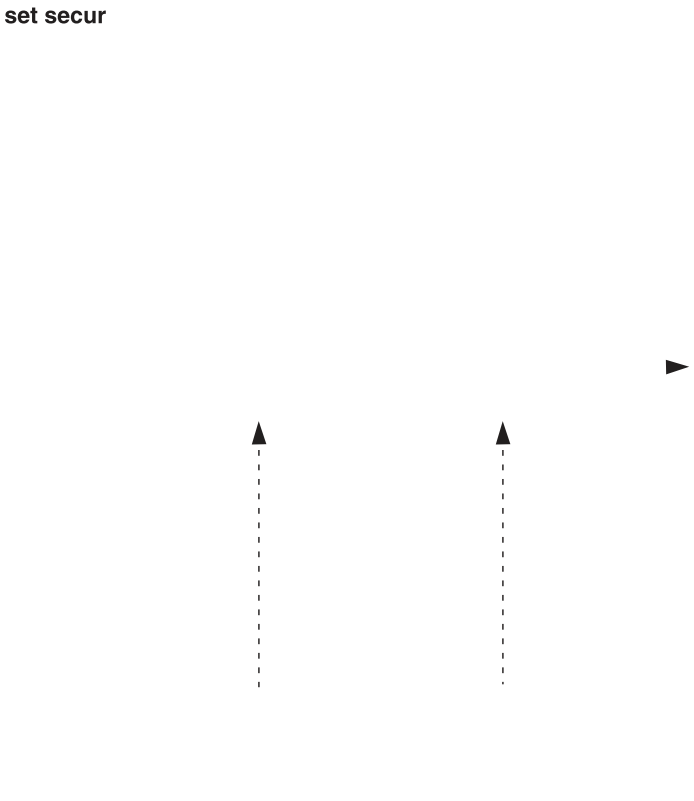
A security access control list (ACL) filters packets for the purpose of discarding them, permitting them, or permitting them with modification (marking) for class-of-service (CoS) priority treatment. A typical use of security ACLs is to enable users to send and receive packets within the local intranet, but restrict incoming packets to the server where confidential salary information is stored.

Trapeze provides a very powerful mapping application for security ACLs. In addition assigning ACLs to physical ports, VLANs, virtual ports in a VLAN, or Distributed MPs, ACLs can be mapped dynamically to a user session, based on authorization information passed back from the AAA server during the user authentication process.

### Overview of Security ACL Commands

**Figure 24–1** provides a visual overview of the way you use MSS commands to set a security ACL, commit the ACL to save the configuration, and map the ACL to a user session, VLAN, port, virtual port, or Distributed MP.

**Figure 24–1. Setting Security ACLs**



- Individual user attribute (**attr filter-id .in** or **attr filter-id .out** is configured on the individual user)
- SSID default (**attr filter-id .in** or **attr filter-id .out** is configured on the SSID service profile)

The user ACL comes from only one of these sources. The sources are listed in order from highest precedence to lowest precedence. For example, if a user associates with an SSID with a default ACL, but a location policy is also applicable to the user, the ACL configured for the location policy is used.

# Creating and Committing a Security ACL

Security ACLs can filter packets by source address, IP protocol, port type, and other characteristics. When you configure an ACE for a security ACL, MSS stores the ACE in the edit buffer until you commit the ACL to be saved to the permanent configuration. You must commit a security ACL before you can apply it to an authenticated user's session or map it to a port, VLAN, virtual port, or Distributed MP. Every security ACL must have a name.

## Setting a Source IP ACL

You can create an ACE that filters packets based on the source IP address and optionally applies CoS packet handling. (For CoS details, see **"Class of Service" on page 24–4**.) You can also determine where the ACE is placed in the security ACL by using the **before** - or **modify** variables with an index number. You can use the **hits** counter to track how many packets the ACL filters.

The simplest security ACL permits or denies packets from a source IP address:

```
set security acl name acl-name {permit [cos cos] | deny}
        {source-ip-addr mask | any}
        [before editbuffer-index | modify editbuffer-index] [hits]
```

For example, to create ACL that permits all packets from IP address 192.168.1.4, type the following command:

```
MX-20#set security acl name acl-1 permit 192.168.1.4 0.0.0.0
```

With the following basic security ACL command, you can specify any of the protocols supported by MSS:

```
set security acl name 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]
```

The following sample security ACL permits all Generic Routing Encapsulation (GRE) packets from source IP address 192.168.1.11 to destination IP address 192.168.1.15, with a precedence level of 0 (routine), and a type-of-service (TOS) level of 0 (normal). (For more information about type-of-service and precedence levels, see the .) GRE is protocol number 47.

```
MX# set security acl name acl-2 permit cos 2 47 192.168.1.11 0.0.0.0 192.168.1.15
        0.0.0.0 precedence 0 tos 0 hits
```

The security ACL F.8( ).3(b)r ACL ( AC)-ingsD[a[(se(lest se□urets )]T7.3D.0807 -1.1024 TD.0017 Tc34002

**Table 24– 1. Common IP Protocol Numbers**

| Number | IP Protocol |
|---|---|
| 1 | Internet Message Control Protocol (ICMP) |
| 2 | Internet Group Management Protocol (IGMP) |
| 6 | Transmission Control Protocol (TCP) |
| 9 | Any private interior gateway (used by Cisco for Internet Gateway Routing Protocol) |
| 17 | User Datagram Protocol (UDP) |
| 46 | Resource Reservation Protocol (RSVP) |
| 47 | Generic Routing Encapsulation (GRE) protocol |
| 50 | Encapsulation Security Payload for IPSec (IPSec-ESP) |
| 51 | Authentication Header for IPSec (IPSec-AH) |
| 55 | IP Mobility (Mobile IP) |
| 88 | Enhanced Interior Gateway Routing Protocol (EIGRP) |
| 89 | Open Shortest Path First (OSPF) protocol |
| 103 | Protocol Independent Multicast (PIM) protocol |
| 112 | Virtual Router Redundancy Protocol (VRRP) |
| 115 | Layer Two Tunneling Protocol (L2TP) |

## Wildcard Masks

When you specify source and destination IP addresses in an ACE, you must also include a wildcard mask for each in the form and

The security ACL checks the bits in IP addresses that correspond to any s (zeros) in the mask, but does not check the bits that correspond to s (ones) in the mask. Specify the IP address and wildcard mask in dotted decimal notation. For example, the IP address and wildcard mask 10.0.0.0 and 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

## Class of Service

Class-of-service (CoS) assignment determines the priority treatment of packets transmitted by an MX, corresponding to a forwarding queue on the MP. **Table 24– 2** shows the results of assigned CoS priorities in security ACLs.

**Table 24– 2. Class-of-Service (CoS) Packet Handling**

| WMM Priority Desired | CLI CoS Value to Enter |
|---|---|
| Background | **1** or **2** |
| Best effort | **0** or **3** |
| Video | **4** or **5** |
| Voice | **6** or **7** |

MP forwarding prioritization occurs automatically for Wi-Fi Multimedia (WMM) traffic. You do not need to configure ACLs to provide WMM prioritization. For non-WMM devices, you can provide MP forwarding prioritization by configuring ACLs.

If you disable WMM, MP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the MP does not tag packets sent to the MX. Otherwise, the classification and tagging described in **"Displaying QoS Information" on page 20–13** remain in effect.

## Creating TCP and UDP ACLs

Security ACLs can filter TCP and UDP packets by source and destination IP address, precedence, and TOS level. You can apply a TCP ACL to established TCP sessions only, not to new TCP sessions. In addition, security ACLs for TCP and UDP can filter packets according to a source port on the source IP address in addition to a destination port on the destination IP address, if yosti(t).1(5 rev28 -1.1T

For example, the following command permits UDP packets sent from IP address 192.168.1.7 to IP address 192.168.1.8, with any UDP destination port less than 65,535. It puts this ACE first in the ACL, and counts the number of hits generated by the ACE.

```
MX# set security acl name acl-5 permit udp 192.168.1.7 0.0.0.0 192.168.1.8 0.0.0.0 lt
        65535 precedence 7 tos 15 before 1 hits
```

(For information about TOS and precedence levels, see the . For CoS details, see **"Class of Service" on page 24–4**.)

### Creating a MAC Address ACL

The following command filters packets based on MAC addresses:

```
MX# set security acl name acl-name {permit|deny} mac {any | src-mac-addr}
        {dest-mac-addr | any | bpdu | broadcast | multicast | pvst}
        ethertype {ethertype-hex | any | arp | ipv4 | ipv6}
```

## Determining the ACE Order

The **set security acl** command creates a new entry in the edit buffer and appends the new entry as a rule at the end of an ACL, unless you specify otherwise. The order of ACEs is significant, because an earlier ACE takes precedence over later ACEs. To place the ACEs in the correct order, use the parameters **before** and **modify** . The first ACE is number 1.

To specify the order of the commands, use the following parameters:

- **before** inserts an ACE before a specific location.
- **modify** changes an existing ACE.

If the security ACL you specify when creating an ACE does not exist when you enter **set security acl ip**, the specified ACL is created in the edit buffer. If the ACL exists but is not in the edit buffer, the ACL reverts, or is rolled back, to the state when its last ACE was committed, but it now includes the new ACE.

For details, see **"Adding Another ACE to a Security ACL" on page 24–12** and **"Modifying an Existing Security ACL" on page 24–13**.

## Committing a Security ACL

To put the security ACLs you have created into effect, use the **commit security acl** command with the name of the ACL. For example, to commit , type the following command:

```
MX# commit security acl name acl-99
success: change accepted.
```

To commit all the security ACLs in the edit buffer, type the following command:

```
MX# commit security acl all
success: change accepted.
```

## Viewing Security ACL Information

To determine whether a security ACL is committed, you can check the edit buffer and the committed ACLs. After you commit an ACL, MSS removes it from the edit buffer.

To display ACLs, use the following commands:

```
show security acl editbuffer
show security acl info all editbuffer
show security acl info
show security acl
```

Use the first two commands to display the ACLs not yet committed to nonvolatile storage. The first command lists the ACLs by name. The second command shows the ACLs in detail.

Use the **show security acl info** command to display ACLs that are already committed. ACLs are not available for mapping until you commit them. (To commit an ACL, use the **commit security acl** command. See **Committing a Security ACL**.)

ACLs do not take effect until you map them to something (a user, Distributed MP, VLAN, port, or virtual port). To map an ACL, see **"Mapping Security ACLs" on page 24–9**. To display the mapped ACLs, use the **show security acl** command, without the **editbuffer** or **info** option.

## Viewing the Edit Buffer

The **editbuffer** command enables you to view the security ACLs you create before committing them to the configuration. To view a summary of the ACLs in the edit buffer, type the following command:

```
MX# show security acl editbuffer
ACL edit-buffer table
ACL                              ype Status
-------------------------------- ---- -------------
acl-99                           IP   Not committed
acl-blue                         IP   Not committed
acl-violet                       IP   Not committed
```

## Viewing Committed Security ACLs

To view a summary of the committed security ACLs in the configuration, type the following command:

```
MX# show security acl
ACL table
ACL                              ype Class  Mapping
-------------------------------- ---- ------ -------
acl-2                            IP   Static
acl-3                            IP   Static
acl-4                            IP   Static
```

## Viewing Security ACL Details

You can display the contents of one or all security ACLs that are committed. To display the contents of all committed security ACLs, type the following command:

```
MX# show security acl info
ACL information for all
set security acl ip acl-999 (hits #2 0)
--------------------------------------------------
 1. deny IP source IP 192.168.0.1 0.0.0.0 destination IP any
 2. permit IP source IP 192.168.0.2 0.0.0.0 destination IP any enable-hits
set security acl ip acl-2 (hits #1 0)
--------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0 destination IP
        192.168.1.15 0.0.0.0 precedence 0 tos 0 enable-hits
You can also view a specific security ACL. For example, to view acl-2, type the fol-
        lowing command:
MX# show security acl info acl-2
ACL information for acl-2
set security acl ip acl-2 (hits #1 0)
--------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0 destination IP
        192.168.1.15 0.0.0.0 precedence 0 tos 0 enable-hits
```

## Displaying Security ACL Hits

Once you map an ACL, you can view the number of packets it has filtered, if you included the keyword **hits**. (For information on setting hits, see **"Setting a Source IP ACL" on page 24–3**.) Type the following command:

```
MX# show security acl hits
ACL hit-counters
Index Counter              ACL-name
----- -------------------- --------
    1                    0 acl-2
    2                    0 acl-999
    5                  916 acl-123
```

To sample the number of hits the security ACLs generate, you must specify the number of seconds between samples. For example, to sample the hits generated every 180 seconds, type the following commands:

```
MX# set security acl hit-sample-rate 180
MX# show security acl hits
ACL hit-counters
```

The security ACL mapped by Filter-Id instructs the MX to use the local definition of the ACL, including the flow direction, to filt

to virtual ports 1 through 3 and 5 on port 2 to filter incoming packets, type the following command:

```
MX# set security acl name map acl-222 port 2 tag 1-3,5 in
```

```
1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0 destination IP 192.168.1.15
        0.0.0.0 precedence 0 tos 0 enable-hits
```

**2.** To add theede2 Tw[( )-6.6(1.)6.7( )-6.6(pe)6.7(rmit L4 Protoco)6.7(l )-6.6(1)6.7(1-6.6(1)6.7(041 Tc  TD.0021)-

## Clearing Security ACLs from the Edit Buffer

Use the **rollback** command to clear changes made to the security ACL edit buffer since it was last committed. The ACL is rolled back to its state at the last **commit** command. For example, suppose you want to remove an ACE that you just created in the edit buffer for :

1. To display the contents of all committed security ACLs, type the following command:

```
MX# show security acl info
ACL information for all
set security acl ip acl-111 (hits #4 0)
----------------------------------------------------
 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
set security acl ip acl-2 (hits #1 0)
----------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0 destination IP
        192.168.1.15 0.0.0.0 precedence 0 tos 0 enable-hits
```

2. To view a summary of the security ACLs for which you just created ACEs in the edit buffer, type the following command:

```
MX# show security acl editbuffer
ACL edit-buffer table
ACL                             ype Status
------------------------------ ---- --------------
acl-a                          IP   Not committed
acl-111                        IP   Not committed
```

3. 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
```

4. To clear the uncommitted ACE from the edit buffer, type the following command:

```
MX# rollback security acl acl-111
```

5. To ensure that you have cleared the ACE, type the following command. Only the uncommitted now appears.

```
MX# show security acl info all editbuffer
ACL edit-buffer information for all
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
```

6. Alternatively, to clear the entire edit buffer of all changes made since a security ACL was last committed and display the results, type the following commands:

```
MX# rollback security acl all
MX# show security acl info all editbuffer
ACL edit-buffer information for all
```

# Using ACLs to Change CoS

For WMM or non-WMM traffic, you can change a packet priority by using an ACL to change the CoS value of the packet. A CoS value assigned by an ACE overrides the CoS value assigned by the MX QoS map.

To change CoS values using an ACL, you must map the ACL to the outbound traffic direction on an MP port, Distributed MP, or user VLAN.

For example, to remap IP packets from IP address 10.10.20.5 with IP precedence value 3, to have CoS value 7 when they are forwarded to any 10.10.30.x address on Distributed MP 2, enter the following commands:

```
MX# set security acl name acl1 permit cos 7 ip 10.10.20.5 0.0.0.0 10.10.30.0
         0.0.0.255 precedence 3
success: change accepted.
MX# set security acl name acl1 permit any
success: change accepted.
MX# commit security acl acl1
success: change accepted.
MX# set security acl name acl1 map ap 2 out
success: change accepted.
```

The default action on an interface and traffic direction that has at least one access control entry (ACE) configured, is to deny all traffic that does not match an ACE on that interface and traffic direction. The **permit any** ACE ensures that traffic that does not match the first ACE is permitted. Without this additional ACE at the end, traffic that does not match the other ACE is dropped.

## Filtering Based on DSCP Values

You can configure an ACE to filter based on a packet Differentiated Services Code Point (DSCP) value, and change the packet CoS based on the DSCP value. A CoS setting marked by an ACE overrides the CoS setting applied from the MX QoS map.

**Table 24– 2** lists the CoS values to use when reassigning traffic to a different priority. The CoS determines the MP forwarding queue to use for the traffic when sending it to a wireless client.

**Table 24– 4. Class-of-Service (CoS) Packet Handling**

| WMM Priority Desired | CLI CoS Value to Enter |
|---|---|
| Background | **1** or **2** |
| Best effort | **0** or **3** |
| Video | **4** or **5** |
| Voice | **6** or **7** |

## Using the dscp Option

The easiest way to filter based on DSCP is to use the **dscp** option. The following commands remap IP packets from IP address 10.10.50.2 that have DSCP value 46 to have CoS value 7 when they are forwarded to any 10.10.90.x address on Distributed MP 4:

```
MX# set security acl name acl2 permit cos 7 ip 10.10.50.2 0.0.0.0 10.10.90.0
         0.0.0.255 dscp 46
success: change accepted.
MX# set security acl ip acl2 permit any
success: change accepted.
MX# commit security acl acl2
success: change accepted.
MX# set security acl map acl2 ap 4 out
success: change accepted.
```

### Using the Precedence and ToS Options

You also can indirectly filter on DSCP by filtering on both the IP precedence and IP ToS values of a packet. However, this method requires two ACEs. To use this method, specify the combination of precedence and ToS values that is equivalent to the DSCP value. For example, to filter based on DSCP value 46, configure an ACL that filters based on precedence 5 and ToS 12. (To display a table of the precedence and ToS combinations for each DSCP value, use the **show qos dscp-table** command.)

The following commands perform the same CoS reassignment as the commands in **"Using the dscp Option" on page 24–15**. They remap IP packets from IP address 10.10.50.2 that have DSCP value 46 (equivalent to precedence value 5 and ToS value 12), to have CoS value 7 when they are forwarded to any 10.10.90.x address on Distributed MP 4:

```
MX# set security acl name acl2 permit cos 7 ip 10.10.50.2 0.0.0.0 10.10.90.0
        0.0.0.255 precedence 5 tos 12
success: change accepted.
MX# set security acl name acl2 permit cos 7 ip 10.10.50.2 0.0.0.0 10.10.90.0
        0.0.0.255 precedence 5 tos 13
success: change accepted.
MX# set security acl name acl2 permit any
success: change accepted.
MX# commit security acl acl2
success: change accepted.
MX# set security acl name acl2 map ap 4 out
success: change accepted.
```

The ACL contains two ACEs. The first ACE matches on precedence 5 and ToS 12. The second ACE matches on precedence 5 and ToS 13. The IP precedence and ToS fields use 7 bits, while the DSCP field uses only 6 bits. Following the DSCP field is a 2-bit ECN field that can be set by other devices based on network congestion. The second ACE is required to ensure that the ACL matches regardless of the value of the seventh bit.


## Enabling Prioritization for Legacy Voice over IP

MSS supports Wi-Fi Multimedia (WMM). WMM support is enabled by default and is automatically used for priority traffic between WMM-capable devices.

MSS also can provide prioritization for non-WMM VoIP devices. However, to provide priority service to non-WMM VoIP traffic, you must configure static CoS or configure an ACL to set the CoS for the traffic. The MP maps the CoS value assigned by static CoS or the ACL to a forwarding queue. The examples in this section show how to configure CoS using ACLs. To use static CoS instead, see **"Configuring Session Timers" on page 20–12**.

### General Guidelines

Trapeze Networks recommends that you follow these guidelines for any wireless VoIP implementation:

- Ensure end-to-end priority forwarding by making sure none of the devices that forward voice traffic resets IP ToS or Diffserv values to 0. Some devices, such as some types of Layer 2 switches with basic Layer 3 awareness, reset the IP ToS or Diffserv value of packets to 0.

MSS uses IP ToS values to prioritize voice traffic. For example, when an MP receives traffic from an MX, the MP classifies the traffic based on the IP ToS value in the IP header of the tunnel carrying the traffic. By default, the MX marks egress traffic for priority forwarding only if WMM is enabled and only if the ingress traffic was marked for priority forwarding. If another forwarding device in the network resets a voice packet priority by changing the IP ToS or Diffserv value to 0, the MX does not reclassify the packet, and the packet does not receive priority forwarding on the MP.

- For WMM-capable devices, leave WMM enabled.
- For SVP devices, change the QoS mode to **svp**. You also need to disable IGMP snooping, and configure an ACL that marks egress traffic from the voice VLAN with CoS value 7. (See **"Enabling SVP Optimization for SpectraLink Phones" on page 24–18** for complete configuration guidelines.)

For other types of non-WMM devices, you do not need to change the QoS mode, but you must configure an ACL to mark the traffic CoS value. This section shows examples for configuring VoIP for devices that use TeleSym, and for Avaya devices.

**Table 24– 5** shows how WMM priority information is mapped across the network. When WMM is enabled in MSS, MX switches and MPs perform these mappings automatically.

You must map the ACL to the outbound traffic direction on an MP port, Distributed MP, or user VLAN. An ACL can set a packet's CoS only in these cases.

You can enable legacy VoIP support on a VLAN, port group, port list, virtual port list, Distributed MP, or user glob. You do not need to disable IGMP snooping.

**MP, vst(mapping)6(pr)TJTwasCon-.1(nf)-4.CL to mark 4.CL Coneo for**

## Enabling SVP Optimization for SpectraLink Phones

The SpectraLink Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SVP phones and WLAN infrastructure products. Trapeze Networks MX switches and MPs are VIEW certified. This section describes how to configure MXs and MPs for SVP phones.

Trapeze Networks recommends that you plan for a maximum of 6 wireless phones per MP.

To configure MSS for SVP phones, perform the following configuration tasks:

- Configure a service for the voice SSID. The service profile also specifies the encryption parameters and attributes for the SSID. This section shows configuration examples for WPA and for RSN (WPA2).
- Configure a radio profile to manage the radios that provide service for the voice SSID.
- Configure a VLAN for the voice clients.
- Configure an authentication and accounting rule that allows clients of the voice SSID onto the network and places them in the voice VLAN.
- Configure an ACL that marks ingress and egress traffic to and from the voice VLAN with CoS value 7.

### Known Limitations

- You cannot have WPA and WPA2 configured on handsets simultaneously within the same ESSID. SVP phones do not check-in.
- You must disable IGMP snooping when running the SpectraLink SRP protocol. SRP uses multicast packets to check-in which are not forwarded through the MX when IGMP snooping is enabled. When a tunneled VLAN is configured over a Layer 3 network, IGMP snooping must be disabled each time the tunnel is established, because the virtual VLAN is established with IGMP snooping enabled by default.

### Configuring a Service Profile for RSN (WPA2)

To configure a service profile for SVP phones that use RSN (WPA2):

- Create the service profile and add the voice SSID to it.
- Enable the RSN information element (IE).
- Disable TKIP and enable CCMP.
- Disable 802.1X authentication and enable preshared key (PSK) authentication instead.
- Enter the PSK key.
- Set the service profile VLAN attribute to the name of the VLAN created for the voice clients.

The following commands configure a service profile called for RSN:

```
MX# set service-profile vowlan-wpa2 ssid-name phones
MX# set service-profile vowlan-wpa2 rsn-ie enable
MX# set service-profile vowlan-wpa2 cipher-tkip disable
MX# set service-profile vowlan-wpa2 cipher-ccmp enable
MX# set service-profile vowlan-wpa2 auth-dot1x disable
MX# set service-profile vowlan-wpa2 auth-psk enable
MX# set service-profile vowlan-wpa2 psk-raw
          c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
MX# set service-profile vowlan-wpa2 attr vlan-name v1
```

### Configuring a Service Profile for WPA

To configure a service profile for SVP phones that use WPA:

- Create the service profile and add the voice SSID.
- Enable the WPA information element (IE). This also enables TKIP. Leave TKIP enabled.
- Disable 802.1X authentication and enable preshared key (PSK) authentication instead.
- Enter the PSK key.

- Set the service profile VLAN attribute to the name of the VLAN you create for the voice clients.

The following commands configure a service profile called for RSN:

```
MX# set service-profile vowlan-wpa ssid-name phones
MX# set service-profile vowlan-wpa wpa-ie enable
MX# set service-profile vowlan-wpa auth-dot1x disable
MX# set service-profile vowlan-wpa auth-psk enable
MX# set service-profile vowlan-wpa psk-raw
          c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
MX# set service-profile vowlan-wpa attr vlan-name v1
```

## Configuring a Radio Profile

MSS has a default radio profile, which manages all radios by default. Some of the radio parameters require changes for voice traffic. You can modify the default radio profile or create a new one.

To create or modify a radio profile for voice clients:

- Map the service profile you created for the voice SSID to the radio profile.
- Change the delivery traffic indication map (DTIM) interval to 3.
- Change the QoS mode to SVP. (This also disables WMM.)
- Configure MPs, if not already configured.
- Map radios to the radio profile and enable them.

The following commands modify the default radio profile for SVP phones:

```
MX# set radio-profile default service-profile vowlan-wpa2
MX# set radio-profile default dtim-interval 3
MX# set radio-profile default qos-mode svp
```

The MP radios are already in the default radio profile by default, so they do not need to be explicitly added to the profile. However, if you create a new radio profile for voice clients, you need to disable the radios, map them to the new radio profile, then reenable them.

## Configuring a VLAN for Voice Clients

MSS requires all clients to be authenticated by RADIUS or the local database, and to be authorized for a specific VLAN. MSS plac

### Disabling RF Auto-Tuning Before Upgrading a SpectraLink Phone

If you plan to upgrade a SpectraLink phone using TFTP over an MP, Trapeze Networks recommends that you disable RF Auto-Tuning before you begin the upgrade. This feature can increase the length of time required for the upgrade. You can disable RF Auto-Tuning on a radio-profile basis. Use the following commands:

```
set radio-profile name auto-tune channel-config disable
set radio-profile name auto-tune power-config disable
```

## Restricting Client-To-Client Forwarding Among IP-Only Clients

You can use an ACL to restrict clients in a VLAN from communicating directly at the IP layer. Configure an ACL that has ACEs to permit traffic to and from the default router (gateway), an ACE that denies traffic between all other addresses within the subnets, and another ACE that allows traffic that does not match the other ACEs.

For example, to restrict client-to-client forwarding within subnet 10.10.11.0/24 in VLAN with default router 10.10.11.8, perform the following steps:

**profile basis. Us**

# Security ACL Configuration Scenario

The following scenario illustrates how to create a security ACL named that consists of one ACE to permit incoming packets from one IP address, and how to map the ACL to a port and a user:

**1.** Type the following command to create and name a security ACL and add an ACE to it.

```
MX# set security acl name acl-99 permit 192.168.1.1 0.0.0.0
```

**2.** To view the ACE you have entered, type the following command:

```
MX# show security acl name editbuffer
ACL                                ype Status
---------------------------------- ---- -------------
acl-99                             IP   Not committed
```

**3.** To save and its associated ACE to the configuration, type the following command:

```
MX# commit security acl name acl-99
success: change accepted.
```

**4.** To map to port 9 to filter incoming packets, type the following command:

```
MX# set security acl name acl-99 map port 9 in
mapping configuration accepted
```

Because every security ACL includes an implicit rule denying all traffic that is not permitted, port 9 now accepts packets only from 192.168.1.1, and denies all other packets.

**5.** To map to user sessions when you are using the local MX database for authentication, configure Natasha in the database with the Filter-Id attribute. Type the following commands:

```
MX# set authentication dot1x user local
success: change accepted.
MX# set user user attr filter-id acl-99.in
success: change accepted.
```

**6.** Alternatively, you can map to user sessions when you are using a remote RADIUS server for authentication. To configure the user for pass-through authentication to the RADIUS server , type the following command:

```
MX# set authentication dot1x user pass-through shorebirds
success: change accepted.
```

You must then map the security ACL to the user session in RADIUS. For instructions, see the documentation for your RADIUS server.

**7.** To save your configuration, type the following command:

```
MX# save config
success: configuration saved.
```

# Part 8 - Configuring Third Party Applications

# Configuring SODA Endpoint Security

Sygate On-Demand (SODA) is an endpoint security solution that allows enterprises to enforce security policies on client devices without installing any special software on the client computers. MSS can be configured to run SODA security checks on computer as a requirement for gaining access to the network.

## About SODA Endpoint Security

The SODA endpoint security solution consists of six modules that provide on-demand security:

- **Virtual Desktop** – Protects confidential data by virtualizing the desktop, applications, file-system, registry, printing, removable media, and copy/paste functions. All data is encrypted on-the-fly and can optionally be erased upon session termination. The virtual desktop is isolated from the normal desktop, protecting the session from previous infection.
- **Host Integrity** – Tests the security of the desktop to determine the level of access to network resources that the device should be granted. Host integrity checks include:
  - Ensuring that an anti-virus product is running with up-to-date virus definitions.
  - Ensuring that a personal firewall is active.
  - Checking that service pack levels are met.
  - Ensuring that critical patches are installed.

  Custom checks can be implemented based on the existence of specific registry keys and values, applications, files, or operating system platforms. Network access can also be prevented based on the existence of specific processes.
- **Malicious Code Protection** – Detects and blocks keystroke loggers that capture usernames and passwords, Trojans that create back-door user accounts, and Screen Scrapers that spy on user activity.

  The Malicious Code module integrates a Virtual Keyboard function that requires users to enter confidential information such as passwords using the Virtual Keyboard when accessing specific Web sites, to protect against hardware keystroke loggers. This module uses a combination of signatures for known exploits and behavioral detection to protect against unknown threats.
- **Cache Cleaner** – Ensures that Web browser information, such as cookies, history, auto-completion data, stored passwords, and temporary files are erased or removed upon termination of the user session, inactivity timeout, or closing of the browser.
- **Connection Control** – Controls network connections based on Domain, IP address, Port, and Service. For example, Connection Control can prevent a Trojan from sending out a confidential document, downloaded legitimately through an SSL VPN tunnel, to a malicious e-mail server (SMTP) using a second network tunnel.
- **Adaptive Policies** – Sense the type and location of device and adjusts access based on endpoint parameters such as IP range, registry keys, and DNS settings

  The SODA endpoint security modules are configured through
  (SODA Manager), a Windows application. SODA Manager is used to create a ,
  which is a Java applet that is downloaded by client devices when they attempt to gain access to the network. Once downloaded, the SODA agent runs a series of security checks to enforce endpoint security on the client device.

## SODA Endpoint Security Support on the MX

The MX supports SODA endpoint security functionality in the following ways:

- SODA agent applets can be uploaded to an MX, stored there, and downloaded by clients attempting to connect to the network.
- The MX can ensure that clients run the SODA agent security checks successfully prior to allowing access to the network.
- Different sets of security checks can be downloaded and run, based on the client SSID.
- If the security checks fail, the MX can deny the client access to the network, or grant the client limited access based on a configured security ACL.
- When the client closes the Virtual Desktop, the MX can disconnect the client from the network.(Optional)

## Configuring SODA MX Switches

This section describes how the SODA functionality is configured to work with an MX, and the procedure that takes place when a user attempts to connect to an SSID where the SODA functionality is enabled.

Note that in the current release, the SODA functionality works only in conjunction with the Web Portal WebAAA feature.

SODA functionality on an MX is configured as follows:

1. Using SODA Manager, a network administrator creates a SODA agent based on the security needs of the network.
2. The network administrator exports the SODA agent files from SODA Manager, and saves them as a .zip file.
3. The SODA agent .zip file is uploaded to the MX using TFTP.
4. The SODA agent files are installed on the MX using a CLI command that extracts the files from the .zip file and places them into a specified directory.
5. SODA functionality is enabled for an SSID configured with Web Portal WebAAA.

Once configured, SODA functionality works as follows:

1. A user connects to an MP managed by a service profile with SODA functionality enabled.
2. Since the Web Portal WebAAA feature is enabled for the SSID, a portal session is started for the user, and the user is placed in the VLAN associated with the **web-portal-*ssid*** or **web-portal-wired** user.
3. The user opens a browser window and is redirected to a login page. And then enters a username and password.
4. The user is redirected to a page called , which exists in the SODA agent directory on the MX.
5. The redirection to the page causes the SODA agent files to be downloaded to the user's computer.
6. Once the SODA agent files have been downloaded, one of the following can take place:
   a. If the MX switch is configured to enforce the SODA agent security checks (the default), then the SODA agent checks are run on the user's computer. If the user's computer passes the checks, then a customizable is loaded in the browser window. The user is then moved from the portal VLAN to his or her configured VLAN and granted access to the network.
   b. If the MX is configured ***not*** to enforce the SODA agent security checks, then the user is moved from the portal VLAN to a configured VLAN and granted access to the network, without waiting for the SODA agent checks to be completed.
   c. If the user's computer fails one of the SODA agent checks, then a customizable is loaded in the browser window. The user is then disconnected from the network, or can

7. At the completion of his or her session, the user can close the SODA Virtual Desktop or point to an advertised logout URL. Either of these actions cause a customizable to be loaded in the browser window. Accessing the logout page causes the user to be disconnected from the network.

## Configuring SODA Functionality

Configuring SODA functionality on an MX consists of the following tasks:

1. Configure Web Portal WebAAA for the service profile. See **"Configuring Web Portal WebAAA for the Service Profile" on page 25–3**.
2. Using SODA manager, create the SODA agent. See **"Creating the SODA Agent with SODA Manager" on page 25–3**.
3. Copy the SODA agent to the MX switch. **"Copying the SODA Agent to the MX" on page 25–4**
4. Install the SODA agent files W 1f (SO)]TJ46.960084 TD.001 TD.3024 Twdironnory(e" on ng thSO)]7.61450

## Enabling SODA Functionality for the Service Profile

To enable SODA functionality for a service profile, use the following command:

```
set service-profile name soda mode {enable | disable}
```

When SODA functionality is enabled for a service profile, a SODA agent is downloaded to clients attempting to connect to an MP managed by the service profile. The SODA agent performs a series of security-related checks on the client. By default, enforcement of SODA agent checks is enabled, so that a connecting client must pass the SODA agent checks in order to gain access to the network.

For example, the following command enables SODA functionality for service profile :

```
MX# set service-profile sp1 soda mode enable
success: change accepted.
```

## Disabling Enforcement of SODA Agent Checks

When SODA functionality is enabled for a service profile, by default the SODA agent checks are downloaded to a client and run before the client is allowed on the network. You can optionally disable the enforcement of the SODA security checks, so that the client is allowed access to the network immediately after the SODA agent is downloaded, rather than waiting for the security checks to be run.

To disable (or re-enable) the enforcement of the SODA security checks, use the following command:

```
set service-profile name enforce-checks {enable | disable}
```

For example, the following command disables the enforcement of the SODA security checks, allowing network access to clients after they have downloaded the SODA agent, but without requiring that the SODA agent checks be completed:

```
MX# set service-profile sp1 enforce-checks disable
success: change accepted.
```

Note that if you disable the enforcement of the SODA security checks, you cannot apply the success and failure URLs to client devices. In addition, you should not configure the SODA agent to refer to the success and failure pages on the MX if you have disabled enforcement of SODA agent checks.

## Specifying a SODA Agent Success Page

When a client successfully runs the checks performed by the SODA agent, by default a dynamically generated page is displayed on the client indicating that the checks succeeded. You can optionally create a custom success page that is displayed on the client instead of the dynamically generated one.

To specify a page to load when a client passes the security checks performed by the SODA agent, use the following command:

```
set service-profile name soda success-page page
```

To reset the success page to the default value, use the following command:

```
clear service-profile name soda success-page
```

The refers to a file on the MX. After this page is loaded, the client is placed in the assigned VLAN and granted access to the network.

For example, the following command specifies , which is a file in the root directory on the MX switch, as the page to load when a client passes the SODA agent checks:

```
MX# set service-profile sp1 soda success-page success.html
success: change accepted.
```

The following command specifies , in the directory on the MX, as the page to load when a client passes the SODA agent checks:

```
MX# set service-profile sp1 soda success-page soda-files/success.html
success: change accepted.
```

## Specifying a SODA Agent Failure Page

When the SODA agent checks fail, by default a dynamically generated page is displayed on the client indicating that the checks failed. You can optionally create a custom failure page that is displayed on the client instead of the dynamically generated one.

To specify a page that is loaded when a client fails the security checks performed by the SODA agent, use the following command:

`set service-profile` *`name`* `soda failure-page` *`page`*

To reset the failure page to the default value, use the following command:

`clear service-profile` *`name`* `soda failure-page`

The refers to a file on the MX switch. After this page is loaded, the specified remediation ACL takes effect, or if there is no remediation ACL configured, then the client is disconnected from the network.

For example, the following command specifies a file in the root directory on the MX, as the page to load when a client fails the SODA agent checks:

```
MX# set service-profile sp1 soda failure-page failure.html
success: change accepted.
```

The following command specifies in the directory on the MX, as the page to load when a client fails the SODA agent checks:

```
MX# set service-profile sp1 soda failure-page soda-files/failure.html
success: change accepted.
```

## Specifying a Remediation ACL

If the SODA agent checks fail on a client, by default the client is disconnected from the network. Optionally, you can specify a failure page for the client to load (with the **set service-profile soda failure-page** command, described above). You can optionally specify a to apply to the client when the failure page is loaded. The remediation ACL can be used to grant the client limited access to network resources, for example.

To specify a remediatito ne

## Specifying a SODA Agent Logout Page

When a client closes the SODA virtual desktop, the client is automatically disconnected from the network. You can optionally specify a page to load when the client logs out of the network. To do this, use the following command:

```
set service-profile name soda logout-page page
```

To reset the logout page to the default value, use the following command:

```
clear service-profile name soda logout-page
```

The refers to a file on the MX.

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 following command:

```
set ip https server enable
```

The client can request the logout page at any time, to ensure that the client session is terminated. You can add the IP address of the MX to the DNS server as a well-known name, and you can advertise the URL of the page to users as a logout page.

For example, the following command specifies a file in the root directory on the MX, 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 on the MX, as the page to load when a client closes the SODA virtual desktop:

```
MX# set service-profile sp1 soda logout-page soda-files/logout.html
success: change accepted.
```

During authentication, a window appears behind the client browser. The window contains a button labeled “End Session”. The client can click this button to terminate the session.

## Specifying an Alternate SODA Agent Directory for a Service Profile

By default, the MX expects SODA agent files for a service profile to be located in a directory with the same name as the SSID configured for the service profile. You can optionally specify a different directory for the SODA agent files used for a service profile. To do this, use the following command:

```
set service-profile name soda agent-directory directory
```

To reset the SODA agent directory to the default value, use the following command:

```
clear service-profile name soda agent-directory
```

If the same SODA agent is used for multiple service profiles, you can specify a single directory for SODA agent files on the MX, rather than placing the same SODA agent files in a separate directory for each service profile.

For example, the following command specifies as the location for SODA agent files for service profile sp1:

```
MX# set service-profile sp1 soda agent-directory soda-agent
success: change accepted.
```

## Uninstalling the SODA Agent Files from the MX

To remove the directory on the MX that contains SODA agent files, use the following command:

```
uninstall soda agent agent-directory directory
```

This command removes the SODA agent directory and all of its contents. All files in the specified directory are removed. The command removes the directory and its contents, regardless of whether it contains SODA agent files.

For example, the following command removes the directory and all of its contents:

```
MX# uninstall soda agent agent-directory sp1
 his will delete all files in agent-directory, do you wish to continue? (y|n) [n]y
```

## Displaying SODA Configuration Information

To view information about the SODA configuration for a service profile, use the **show service profile** command.

# Configuring Location Based Services

AeroScout RFID tags are wireless transmitters placed on assets such as office equipment to track the equipment location. Each tag regularly transmits a unique ID. AeroScout listeners detect the transmissions from the RFID tags and relay this information to an AeroScout Engine or an MX. You can use an AeroScout Engine or RingMaster to locate the asset.

MPs can be configured as AeroScout listeners. An MP configured as an AeroScout listener detects RFID tag IDs and sends the tag information to the MX managing the MP. If an AeroScout Engine is configured to request the information from the MP, the MP also sends the information to the AeroScout Engine.

The accuracy of the location information depends on the number of listeners (MPs). Trapeze Networks recommends that you configure at least three listeners.


## Configuring MP Radios to Listen for AeroScout RFID Tags

To configure MP radios to listen for AeroScout RFID tags:

- Configure a service profile for the AeroScout listeners and set the SSID type to clear (unencrypted).
- Configure a radio profile for the AeroScout listeners.
  - Disable RF Auto-Tuning of channels on the radio profile. Channels on RFID tags are statically configured. Therefore, the listener should not dynamically change channels.
  - Disable active scan on the radio profile. When active scan is enabled, radios go off-channel for brief intervals to scan for rogues.
  - Enable RFID mode on the radio profile. RFID mode allows MP radios to accept Aeroscout Engine commands. An MP forwards RFID tags to an Aeroscout Engine after receiving an Enable Access Point command from the Aeroscout Engine.
  - Map the AeroScout listeners service profile to the radio profile.
  - Set the channel on each radio to the channel on which the RFID tags transmit. You can use the same channel on all the RFID tags.
  - Map the MP radios to the radio profile and enable the radios.

The following example shows the commands to configure three MPs to be AeroScout listeners. This example assumes that the MPs have already been installed and configured.

```
MX# set service-profile rfid-listeners ssid-type clear
success: change accepted.
MX# set radio-profile rfid-listeners active-scan disable
success: change accepted.
MX# set radio-profile rfid-listeners auto-tune channel-config disable
success: change accepted.
MX# set radio-profile rfid-listeners rfid-mode enable
success: change accepted.
MX# set radio-profile rfid-listeners service-profile rfid-listeners
success: change accepted.
MX# set ap 67 radio 1 channel 7
success: change accepted.
MX# set ap 68 radio 1 channel 7
success: change accepted.
MX# set ap 69 radio 1 channel 7
success: change accepted.
MX# set ap 67 radio 1 radio-profile rfid-listeners mode enable
success: change accepted.
MX# set ap 68 radio 1 radio-profile rfid-listeners mode enable
success: change accepted.
MX# set ap 69 radio 1 radio-profile rfid-listeners mode enable
success: change accepted.
```

# Locating an RFID Tag

You can use an AeroScout Engine or RingMaster to locate an asset with an attached RFID tag.

## Using an AeroScout Engine

1. Load the site map in AeroScout System Manager.
2.

27

# AirDefense Integration with Trapeze Mobility System

This chapter describes how the AirDefense security system integrates with the Trapeze Mobility System, and how a Trapeze Mobility Point can be converted into an AirDefense sensor.

## About AirDefense Integration

The AirDefense system is an enterprise-class security solution that allows you to protect against threats and intrusions into your wireless network. The AirDefense solution can be integrated with the Trapeze Mobility System, complementing Trapeze network security features by providing a centralized server dedicated to security analysis and record keeping.

AirDefense constantly monitor the network, relaying information to a central AirDefense collects and analyzes the information. RingMaster can be configured to receive alert information from the AirDefense server.

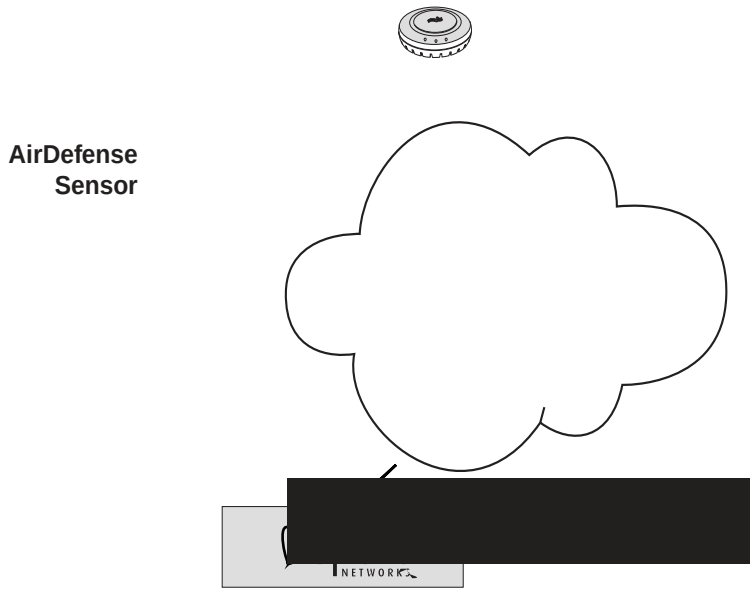
The AirDefense security solution can detect and report when events such as the following occur:

- An attacker sends spoofed deauthentication or disassociation frames to clients in the network.
- An attacker spoofs client MAC addresses to flood the network with traffic and create a denial of service attack.
- An unauthorized access point appears in the network.
- Excessive traffic is observed between wireless clients.
- An excessive number of decryption errors are observed.
- A NetStumbler scan is detected on the network.

The Trapeze Mobility System integrates with the AirDefense security solution in the following ways:

-

**Figure 27–1. AirDefense Integration with the Trapeze Mobility System**




In the example above, an MP converted to an AirDefense sensor monitors the network and sends information to the AirDefense server, via an MX. The AirDefense server analyzes the information received from the sensors and relays SNMP traps to the RingMaster server, where they can be viewed as alarms by RingMaster clients.

# Converting an MP into an AirDefense Sensor

This section describes the procedures for converting an MP into an AirDefense sensor, specifying the AirDefense server the converted MP sends information to, and how to convert an AirDefense sensor back to an MP.

The following tasks are described:



## Copying the AirDefense Sensor Software to the MX

The AirDefense sensor software is contained in a file called . After obtaining the AirDefense sensor software, copy the file to the MX managing the MP to be converted to an AirDefense sensor.

For example, the following command copies the file from a TFTP server to the MX switch:

```
MX# copy tftp://172.16.0.1/adconvert.bin adconvert.bin
.................success: received 945572 bytes in 10.090 seconds [ 93713 bytes/
         sec]

success: copy complete.
```

## Loading the AirDefense Sensor Software on the MP

After the AirDefense sensor software is copied to the MX, you can configure an MP to load the software. When you do this, the software is transferred to the MP, which reboots and comes up as an AirDefense sensor.

To configure an MP to load the AirDefense sensor software, use the following command:

```
set ap apnum image filename
```

For example, the following command causes Distributed MP 1 to load the file, then reboot as an AirDefense sensor:

```
MX# set ap 1 image adconvert.bin
 his will change the file a AP will boot. Would you like to continue? (y/n) [n] y
```

### How a Converted MP Obtains an IP Address

If you had previously configured the MP to use a static IP address, and the MP boots as an AirDefense sensor, the MP uses the same IP address. Otherwise, the converted MP uses DHCP to obtain an IP address.


Optionally, the converted MP can obtain an IP address directly from an AirDefense server. To do this, configure your DHCP server to include the IP address or hostname of the AirDefense server in the Option 43 field of the DHCP Offer message. After receiving a DHCP Offer identifying an AirDefense server in the option 43 field, a converted MP contacts the AirDefense server and obtains an IP address from it.

## Specifying the AirDefense Server

To specify the AirDefense server the converted MP sends information to, do the following:

1. Open a Web browser and establish a secure (HTTPS) connection to the converted MP.
2. Using the converted MP Web interface, specify the IP address, subnet mask, and default gateway of the AirDefense server.

After you do this, the converted MP can download a software image from the specified AirDefense server and operate as an AirDefense sensor.

## Converting an AirDefense Sensor Back to an MP

Once an MP is converted to an AirDefense sensor, you can return the MP to a Trapeze Mobility Point by doing the following:

1. Open a Web browser and establish a secure (https) connection to the converted MP.
2. Click Revert in the converted MP Web interface.

When you do this, the MP reboots and comes up as a Trapeze Mobility Point.

## Clearing the AirDefense Sensor Software from the MP Configuration

To clear the AirDefense sensor software file from the MP configuration, use the following command:

```
clear ap apnum image
```

For example, 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.
```

The next time the MP is booted, it becomes a Trapeze Mobility Point.

| | | |
|---|---|---|
| Configuration information disappears after a software reload. | The configuration changes were not saved. | 1. Retype the commands for the missing configuration information.<br>2. Type the **save config** command to save the changes. |
| Mgmt LED is quickly blinking amber.<br>CLI stops at boot prompt (boot>). | The MX was unable to load the system image file. | Type the **boot** command at the boot prompt. |

# Recovering the System After Losing the Enable Password

You can recover any model MX if you have lost or forgotten the enable password. You also can recover an MXR-2 even if you have lost or forgotten the login password.

To recover an MX, use one of the following procedures.

## MXR-2

1. After the MX has fully booted, use a pin to press the factory reset switch for at least 5 seconds. This operation erases the MX configuration.
2. Use a Web browser to access IP address 192.168.100.1. This address accesses the Web Quick Start.
3. Use the Web Quick Start to set the administrator usernames and passwords and other parameters. Make sure you reconfigure the MX IP connection.
4. See **"First-Time Configuration via the Console" on page 6–3**.

## MX-20, MX-200, MX-216 MX-400, or MX-8

1. Reboot the MX, and interrupt the MX boot process.

   Insert a pin into the restart switch or power the MX off and on again to cause the MX to reboot. **Figure A–2** shows the location of the restart switch on an MX-20. The restart switch on an MX-8 or MX-400 is also located next to the serial console port.

**Figure A–2. MX Restart Switch Location**

2. When you see descending numbers on the console, press **q**, then press Enter.
3. Type the following command at the boot> prompt:

```
boot> boot OP +=default
```

If you do not type the command before the reset cycle is complete, the MX returns to the same state before you restarted it.

Once you have entered the command, the MX returns to the initial unconfigured state. For information on how to configure the MX, see **"First-Time Configuration via the Console" on page 6–3**.

For model MX-8, MX-200, or MX-216, you also can reconfigure basic parameters using the Web Quick Start. Use a Web browser to access IP address 192.168.100.1.

# Configuring and Managing the System Log

System logs provide information about system events that you can use to monitor and troubleshoot MSS. Event messages for the MX and the attached MPs can be stored or sent to the following destinations:

- Stored in a local buffer on the MX.
- Displayed on the MX console port.
- Displayed in an active Telnet session.
- Sent to one or more syslog servers, as specified in RFC 3164.

The system log is a file in which the newest record replaces the oldest. These entries are preserved in nonvolatile memory through system reboots.

## Log Message Components

Each log message contains the following components:

## Logging Destinations and Levels

A logging destination is the location that logged event messages are sent for storage or display. By default, only session logging is disabled. You can enable or disable logging to each destination and filter the messages by the severity of the logged event or condition. (For details, see Table A– 3, "Event Severity Levels," on page 4.)

System events and conditions at different severity 4le6671n u26714di491084 T19 42334.00418.e M

To clear log messages from the system or trace buffer, use the following command:

```
clear log buffer | trace
```

To stop sending messages to a syslog server, use the following command:

```
clear log server server-addr
```

## Logging to the Log Buffer

The system log consists of rolling entries stored as a last-in first-out queue maintained by the MX. Logging to the buffer is enabled by default for events at the error level and higher.

To modify settings to another severity level, use the following command:

```
set log buffer severity severity-level
```

For example, to set logging to the buffer for events at the warning level and higher, type the following command:

```
MX# set log buffer severity warning
success: change accepted.
```

To view log entries in the system log buffer, use the following command:

```
show log buffer [{+|-} number-of-messages] [facility facility-name] [matching
         string] [severity severity-level]
```

You can display the most recent messages or the oldest messages:

- Type a positive number (for example, +100) to display that number of log entries starting from

For example, to set logging to the console for events at the critical severity level and higher, type the following command:

```
MX# set log console severity critical
success: command accepted.
```

To disable console logging, type the following command:

```
MX# set log console disable
success: change accepted.
```

## Changing the Current Telnet Session Defaults

By default, log information is not sent to your current Telnet session, and the log level is set to information (info) or higher. To modify the severity of events logged to your current Telnet session, use the following command from within the session:

```
set log current severity severity-level
```

(For information about severity levels, see Table A– 3 on page 4.)

To enable current session logging, type the following command:

```
MX# set log current enable
success: change accepted
```

To disable current session logging, type the following command:

```
MX# set log current disable
success: change accepted
```

## Logging to the Trace Buffer

Trace logging is enabled by default and stores debug-level output in the MX trace buffer. To modify trace logging to an .7(:l)-6(in.006[((For3/F4 1 8uffer.A-1.10s)-6lo)-6.9(gg)-6(in)-4.5(g )-6(to)-6.9( l ouon D

### Displaying the Log Configuration

To display your current log configuration, type the following command:

```
MX# show log config
Logging console:               enabled
Logging console severity:      INFO
Logging sessions:              enabled
Logging sessions severity:     INFO
Logging buffer:                enabled
Logging buffer severity:       ERROR
Logging trace:                 enabled
Logging trace severity:        DEB G
Logging buffer size:           1048576 bytes
Log marking:                   disabled
Log marking severity:          NO ICE
Log marking interval:          300 seconds
Logging server:                172.21.12.19 port 514 severity EMERGENCY
Current session:                 disabled
Current session severity:        INFO
```

## Running Traces

Trace commands enable you to perform diagnostic routines. You can set a trace command with a keyword, such as **authentication** or **sm**, to trace activity for a par

### Tracing Authorization Activity

Tracing authorization activity can help diagnose authorization problems. For example, to trace the authorization of MAC address 00:00:30:b8:72:b0, type the following command:

```
MX# set trace authorization mac-addr 00:00:30:b8:72:b0
success: change accepted.
```

### Tracing 802.1X Sessions

Tracing 802.1X sessions can help diagnose problems with wireless clients. For example, to trace 802.1X activity for user tamara@example.com at level 4, type the following command:

```
MX# set trace dot1x user tamara@example.com level 4
success: change accepted.
```

## Displaying a Trace

Use the **show trace** command to show the trace areas that are enabled. For example, to display all currently running trace commands, type the following command:

```
MX# show trace
milliseconds spent printing traces: 31.945
 race Area           Level Mac                ser              Port Filter
-------------------- ----- ----------------- ---------------- ---- --------
authentication           3                   admin                       0
authorization            5                                               0
sm                       5                                    11         0
dot1x                    2                                               0
```

## Stopping a Trace

The **clear trace** commands deletes running trace commands. To clear all traces or a particular trace area, type the following command:

```
clear trace {all | trace area}
```

(For a list of all areas that can be traced, see **"List of Trace Areas" on page A–10**.)

For example, to stop a trace of session manager activity, type the following command:

```
MX# clear trace sm
success: change accepted.
```

## About Trace Results

The trace commands use the underlying logging mechanism to deliver trace messages. Trace messages are generated with the debug severity level. By default, the only log target that receives debug-level messages is the volatile trace buffer. (To see the contents of the trace buffer, see **"Displaying Trace Results" on page A–10**.)

The volatile trace buffer receives messages for all log severities when any trace area is active. However, if no trace area is active, no messages are sent to the trace buffer regardless of their severity. If you do not enable trace commands, the trace buffer is effectively disabled.

Because traces use the logging facility, any other logging target can be used to capture trace messages if the severity is set to debug. However, since tracing can be voluminous, Trapeze Networks discourages this in practice. To enable trace output to the console, enter the command **set log console severity debug**.

If you attempt to send trace output to a Telnet session, be aware that tracing is disabled for areas processing packets that might be associated with the Telnet session.

## Displaying Trace Results

To view the output of currently running trace commands, use the following command:

```
show log trace [{+|-|/}number-of-messages] [facility facility-name]
         [matching string] [severity severity-level]
```

For example, the following command displays a trace log of error-level events:

```
MX# show log trace severity error
KERNEL Jan 15 23:08:10 ERROR duplicate IP address 10.7.122.102 sent from link
         address 00:05:5d:45:ae:cd
```

To display a specific number of trace log messages, you must enter a plus sign (+), minus sign (-), or slash (/) before the number. These characters filter the messages displayed as follows:

To filter trace output by MSS area, use the **facility** keyword. For a list of valid facilities for which you can view event messages, type the following command:

```
MX# show log trace facility ?
<facility name>            Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP,ASO,
         BOO , CLI, CL S ER, CRYP O, DO 1X, ENCAP, E HERNE , GA EWAY, H  PD, IGMP,
         IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROG E, SM, SNMPD, SPAN, S ORE,
         SYS,  AGMGR,  BRIDGE,  CPSSL,  ELNE ,  F P,  LS,   NNEL, VLAN, X509, XML,
         MP, RAPDA, WEBVIEW, EAP, POR CONFIG, FP.
```

## Copying Trace Results to a Server

To copy the contents of the trace buffTc-D2-mesy ae636759036 0 TD.001 Tc-.0017 TN, 0r2( eR)19rarea, of the foll

## Viewing VLAN Interfaces

To view interface information for VLANs, type the following command:

```
MX-20# show interface
* = From DHCP
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- --------
   1 default         0.0.0.0         0.0.0.0         NO      Down  ipv4
 130 vlan-eng        192.168.12.7    255.255.255.0   YES      p    ipv4
 190 vlan-wep        192.168.19.7    255.255.255.0   YES      p    ipv4
```

(For more information about VLAN interfaces, see **"Configuring and Managing VLANs" on page 7–13**.)

## Viewing AAA Session Statistics

To view AAA session statistics, type the following command:

```
MX# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=5 key=(null) author-pass=(null)
Radius Servers
Server                   Addr           Ports    /o  ries Dead State
-------------------------------------------------------------------
SQA2BServer          11.1.1.11       1812 1813  5    3    5     P
SideShow             192.168.0.21    1812 1813  5    3    0     P
Server groups
    sg1: SideShow
    SQA: SQA2BServer
set authentication dot1x *@xmpl.com pass-through sg1
set authentication dot1x *@xmpl.com pass-through SQA
set authentication dot1x EXAMPLE\* peap-mschapv2 sg1
user sqa
password = 08325d4f (encrypted)
session-timeout = 3600
mac-user 00:00:a6:47:ad:03
session-timeout = 3600
vlan-name = vlan-wep
mac-user 00:00:65:16:0d:69
session-timeout = 3600
vlan-name = vlan-eng
```

(For more information about AAA, see the
.)

## Viewing FDB Information

The **show fdb** command displays the hosts learned by the MX and the ports connected to the hosts. To display forwarding database (FDB) information, type the following command:

```
MX# show fdb
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN  AG  Dest MAC/Route Des [CoS]  Destination Ports or VCs/[Protocol  ype]
---- ---- ------------------ -----  ---------------------------------------
 130    3 00:05:5d:7e:94:83                1                          [ALL]
 130  130 00:02:2d:85:6b:4d                t:192.168.14.6             [ALL]
 130  130 00:0b:0e:12:34:56                t:192.168.15.5             [ALL]
 130  130 00:0b:0e:02:76:f6                t:192.168.14.6             [ALL]
 130    2 00:02:2d:86:bd:38                3                          [ALL]
 130    3 00:05:5d:84:d3:d3                1                          [ALL]
4097      00:0b:0e:00:04:30     #           CP                         [ALL]
4096      00:0b:0e:00:04:30     #           CP                         [ALL]
130      00:0b:0e:00:04:30      #           CP                         [ALL]
 otal Matching FDB Entries Displayed = 32
dynamic = 27, static=0, permanent=0, system=5
```

(For more information about forwarding databases, see **“Managing the Layer 2 Forwarding Database” on page 7–18**.)

## How Remote Traffic Monitoring Works

To monitor wireless traffic, an MP radio compares traffic sent or received on the radio to snoop filters applied to the radio by the network administrator. When an 802.11 packet matches all conditions in a filter, the MP encapsulates the packet in a Tazmen Sniffer Protocol (TZSP) packet and sends the packet to the observer host IP addresses specified by the filter. TZSP uses UDP port 37008 for transport. (TZSP was created by Chris Waters of Network Chemistry.)

You can map up to eight snoop filters to a radio. A filter does not become active until you enable it. Filters and their mappings are persistent and remain in the configuration following a restart. The filter state is also persistent across restarts. Once a filter is enabled, if the MX or the MP is subsequently restarted, the filter remains enabled after the restart. To stop using the filter, you must manually disable it.

### Using Snoop Filters on Radios Configured for Active Scanning

When active scan is enabled in a radio profile, the radios with the profile actively scan other channels in addition to the data channel that is currently in use. Active scan operates on enabled radios and disabled radios. In fact, using a radio in sentry mode as a dedicated scanner provides better rogue detection because the radio can spend more time scanning on each channel.

When a radio is scanning other channels, active snoop filters on the radio also snoop traffic on the other channels. To prevent monitoring of data from other channels, use the **channel** option when you configure the filter, to specify the channel on which you want to snoop.

### All Snooped Traffic Is Sent in the Clear

Traffic that matches a snoop filter is copied after decryption. The decrypted (clear) version is sent to the observer.

## Best Practices for Remote Traffic Monitoring

- Do not specify an observer associated with the MP 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 a 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 running 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 use 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.

  To inform you of this condition, MSS generates a log message such as the following the first time an ICMP error message is received following the start of a snoop filter:

  To prevent ICMP error messages from the observer, Trapeze Networks recommends using the Netcat application on the observer to listen to UDP packets on the TZSP port.

## Configuring a Snoop Filter

To configure a snoop filter, use the following command:

```
set snoop <snoop-filter> [condition-list] [observer ip-addr]
         [snap-length <value> | interval <value> | security]]
```

The  can be up to 15 alphanumeric characters.

The specifies the match criteria for packets. Conditions in the list are appended. Therefore, to be copied and sent to an ob

### Deleting a Snoop Filter

To delete a snoop filter, use the following command:

```
clear snoop filter-name
```

## Mapping a Snoop Filter to a Radio

You can map a snoop filter to a radio on an MP. To map a snoop filter to a radio, use the following command:

```
set snoop map filter-name ap  radio {1 | 2}
```

You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the MP sends only one copy of a packet that matches a filter to the observer. After the first match, the MP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the MP still maintains a counter of the number of packets that match the filter. (See “Displaying Remote Traffic Monitoring Statistics” on page 16.)

The following command maps snoop filter to radio 2 on MP 3:

```
MX# set snoop map snoop1 ap 3 radio 2
success: change accepted.
```

### Displaying the Snoop Filters Mapped to a Radio

To display the snoop filters that are mapped to a radio, use the following command:

```
show snoop map filter-name
```

The following command shows the mapping for snoop filter :

```
MX# show snoop map snoop1
filter 'snoop1' mapping
Ap: 3          Radio: 2
```

### Displaying the Snoop Filter Mappings for All Radios

To display all snoop filter mappings, use the following command:

```
MX# show snoop
Ap: 3          Radio: 2
        snoop1
        snoop2
Ap: 2          Radio: 2
        snoop2
```

### Removing Snoop Filter Mappings

To remove a snoop filter from a specific radio, use the following command:

```
clear snoop map filter-name ap ber radio {1 | 2}
```

The following command removes snoop filter from radio 2 on MP 3:

```
MX# clear snoop map snoop2 ap 3 radio 2
success: change accepted.
```

To remove all snoop filter mappings from all radios, use the following command:

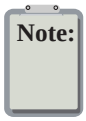
```
clear snoop map all
```

## Enabling or Disabling a Snoop Filter

A snoop filter does not take effect until you enable it. To enable or disable a snoop filter, use the following command:

```
set snoop {filter-name | all} mode {enable | disable}
```

The filter operates until you manually disable it.




The following command enables snoop filter :

```
MX# set snoop snoop1 mode enable
success: filter 'snoop1' enabled
```

## Displaying Remote Traffic Monitoring Statistics

The MP collects statistics for packets matching the enabled snoop filters mapped to the radios. The MP retains statistics for a snoop filter until the filter is changed or disabled. The MP then clears the statistics.

To display statistics for packets matching a snoop filter, use the following command:

```
show snoop stats [filter-name [ [radio {1 | 2}]]]
```

The following command shows statistics for snoop filter :

```
MX# show snoop stats snoop1
Filter          Ap Radio   Rx Match      x Match     Dropped
================================================================================
snoop1            3     1             96            4            0
```

## Preparing an Observer and Capturing Traffic

To observe monitored traffic, install the following applications on the observer:

- Ethereal or Tethereal Version 0.10.8 or later
- Netcat (any version), if not already installed

Ethereal and Tethereal decode 802.11 packets embedded in TZSP without any configuration.

Use Netcat to listen to UDP packets on the TZSP port. This avoids a constant flow of ICMP destination unreachable messages from the observer back to the radio. You can obtain Netcat through the following link:

http://www.vulnwatch.org/netcat/

If the observer is a PC, you can use a Tcl script instead of Netcat if preferred.

1. Install the required software on the observer.
2. Configure and map snoop filters in MSS.
3. Start Netcat:

- On Linux or Unix, use a command such as the following:

```
nc -l -u -p 37008 ip-addr > /dev/null &
```

- On Windows, use the following command:

```
netcat -l -u -p 37008 -v -v
```

Where is the IP address of the Distributed MP with the mapped snoop filter. (To display the Distributed MP IP address, use the **show ap status** command.)

4. Start the capture application:

- For Ethereal capture, use **ethereal filter port 37008**.
- For Tethereal capture, use **tethereal -V port 37008**.

5. Disable the option to decrypt 802.11 payloads. Because the MP always decrypts the data before sending it to the observer, the observer does not need to perform any decryption. In fact, if you leave decryption enabled on the observer, the payload data becomes unreadable.

To disable the decryption option in Ethereal:

**a.** In the decode window, right-click on the line.

**b.** Select **Protocol Preferences**

To copy core files, use the **dir** command to list them, then use the **copy** command to copy them. The following example shows how to list the files and copy them to a TFTP server.

```
MX# dir
================================================================================
file:
Filename                                        Size           Created
file:configuration                              48 KB      Jul 12 2005, 15:02:32
file:sysa_bak                                   12 KB      Mar 15 2005, 19:18:44
 otal:         60 Kbytes used, 207762 Kbytes free
================================================================================
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:  otal:        9780 Kbytes used, 2460 Kbytes free
Boot1:  otal:        9796 Kbytes used, 2464 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
core:command_audit.cur                         37 bytes   Aug 28 2005, 21:11:41
core:netsys.core.217.tar                        560 KB    May 06 2005, 21:48:33
 otal:          560 Kbytes used, 91147 Kbytes free
```

In this example, the core file is netsys.core.217.tar. (The command_audit.cur file is not a core file and is created as part of normal system operation.)

The following command copies the core file onto a TFTP server.

```
MX# copy core:netsys.core.217.tar tftp://192.168.0.233/netsys.core.217.tar
..........success: sent 573440 bytes in 1.431 seconds [ 400726 bytes/sec]

success: copy complete.
```

If the MX network interfaces to the TFTP server are not available, copy the core file to the nonvolatile file area before restarting the MX. The following commands copy netsys.core.217.tar to the nonvolatile file area and verify the result:

```
MX# copy core:netsys.core.217.tar file:netsys.core.217.tar
success: copy complete.
MX# dir
================================================================================
file:
Filename                                        Size           Created

core:netsys.core.217.tar                        560 KB    May 06 2005, 21:48:33
file:configuration                              48 KB     Jul 12 2005, 15:02:32
file:sysa_bak                                   12 KB     Mar 15 2005, 19:18:44
 otal:         620 Kbytes used, 207202 Kbytes free
================================================================================
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:  otal:        9780 Kbytes used, 2460 Kbytes free
Boot1:  otal:        9796 Kbytes used, 2464 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
core:command_audit.cur                         37 bytes   Aug 28 2005, 21:11:41
core:netsys.core.217.tar                        560 KB    May 06 2005, 21:48:33
 otal:          560 Kbytes used, 91147 Kbytes free
```

## Debug Messages

In addition to generating a core file, the MX also sends debug messages to the serial console during a system crash. To capture the messages, attach a PC to the port (if one is not already attached) and use the terminal emulation application on the PC to capture a log of the messages. (For information about connecting to the serial console port, see the
.)

## Sending Information to TAC

After you save the **show tech-support**

# Traffic Ports Used by MSS

When deploying a Trapeze wireless network, you might attach Trapeze equipment to subnets with firewalls or access controls between them. Trapeze equipment uses various protocol ports to exchange information. To ensure full operation of your network, make sure the equipment can exchange information on the ports listed in **Table B– 4**.

**Table B– 4. Traffic Ports Used by MSS**

| Protocol | Port | Function |
|---|---|---|
| IP/TCP (6) | 23 | Telnet management |
| IP/TCP (6) | 443 | SSL management of an MX via Web View<br>Port 443 is also the default port used by RingMaster clients to communicate with a RingMaster server. |
| IP/TCP (6) | 8821 | Network Domain and Mobility Domain management<br>The originating MX connects from a random TCP port equal to or higher than 4096. The target MX listens for the traffic on TCP por 821. |
| IP/TCP (6) | 8889 | SSL management via RingMaster or GuestPass<br>RingMaster or GuestPass originates the SSL connection on TCP port 8889. |
| IP/UDP (17) | 53 | DNS |
| IP/UDP (17) | 123 | NTP |
| IP/UDP (17) | 161 | SNMP get and set operations |
| IP/UDP (17) | 162 | SNMP traps |
| IP/UDP (17) | 1812 | RADIUS authentication (default setting) |
| IP/UDP (17) | 1813 | RADIUS accounting (default setting) |
| IP/UDP (17) | 5000 | MX-MP communication. This applies to MX communication with Distributed MPs and with directly connected MPs. |
| IP/UDP (17) | 5247 | MX-MP communication. This applies to MX communication with Distributed MPs and with directly connected MPs. This includes CAPWAP data. |
| IP/ICMP (1) | N/A | Several types (for example, ping) |

Roaming traffic uses IP tunnels, encapsulated with IP protocol 4.

To list the TCP port numbers in use on an MX, including those for the other end of a connection, use the **show tcp** command.

# Supported RADIUS Attributes

Trapeze Networks Mobility System Software (MSS) supports the standard and extended RADIUS authentication and accounting attributes listed in Table C– 5 on page 1. Also supported are Trapeze Networks vendor-specific attributes (VSAs), listed in Table C– 6 on page 4.

An attribute is sent to RADIUS accounting only if the table listing it shows or in the

| | | | | | |
|---|---|---|---|---|---|
| Service-Type | 5 | No | Yes | Yes | Access type, which can be one of the following:<br>❑ 2—Framed, for network user access<br>❑ 6—Administrative, for administrative access to the MX, with authorization to access the enabled (configuration) mode. The user must enter the **enable** command and the correct enable password to access the enabled mode.<br>❑ 7—NAS-Prompt, for administrative access to the nonenabled mode only. In this mode, the user can still enter the **enable** command and the correct enable password to access the enabled mode.<br>For administrative sessions, the MX always |

| | | | | | | |
|---|---|---|---|---|---|---|
| Acct-Multi-Session-Id | 50 | No | No | Yes | Yes | Unique accounting ID that facilitates linking together multiple related sessions in a log file. Each linked session has a unique Acct-Session-Id but the same Acct-Multi-Session-Id. |
| Acct-Input-Gigawords | 52 | No | No | Yes | | Number of times the Acct-Input-Octets |

## Trapeze Networks Vendor-Specific Attributes

The vendor-specific attributes (VSAs) created by Trapeze Networks are embedded according to the procedure recommended in RFC 2865, with Vendor-ID set to 14525. **Table C– 6** describes the Trapeze Networks VSAs, listed in order by vendor type number.

(For attribute details, see Table 11– 5, “Authentication Attributes for Local Users,” on page 34.)

| | | | | | | |
|---|---|---|---|---|---|---|
| Encryption-Type | 26, 14525, 3 | Yes | No | No | Yes | Type of encryption used to authenticate the client. |
| Time-Of-Day | 26, 14525, 4 | Yes | No | No | Yes | Day(s) and time(s) during which a user can log into the network. |
| SSID | 26, 14525, 5 | Yes | No | Yes | Yes | Name of the SSID for the user. 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. |
| End-Date | 26, 14525, 6 | | | | | |

# Managing Keys and Certificates

A digital certificate is a form of electronic identification for network applications and equipment. The MX requires digital certificates to authenticate communications to RingMaster and Web View, WebAAA clients, and 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, servers, and wireless clients to exchange information secured by encryption.

## Why Use Keys and Certificates?

Certain MX operations require the use of public-private key pairs and digital certificates. All RingMaster and Web View users, and users configured for IEEE 802.1X EAP authentication or WebAAA, require public-private key pairs and digital certificates to be installed on the MX switch.

These keys and certificates are fundamental to securing wireless, wired authentication, and administrative connections because they support Wi-Fi Protected Access (WPA) encryption and dynamic Wired-Equivalency Privacy (WEP) encryption.

### Wireless Security through TLS

In the case of wireless or

1. To form the encrypted TLS channel, the MX must have a digital certificate and must send that certificate to the wireless client.
2. Inside the MX digital certificate is the MX public key, that the wireless client uses to encrypt a pre-master secret key.
3. The wireless client then sends the key back to the MX so that both the MX and the client can derive a key from this pre-master secret for secure authentication and wireless session encryption.

Clients authenticated by PEAP need a certificate in the MX only when the MX performs PEAP locally, not when EAP processing takes place on a RADIUS server. (For details about authentication options, see the

.

# About Keys and Certificates

Public-private key pairs and digital signatures and certificates allow keys to be generated dynamically so that data can be securely encrypted and delivered. You generate the key pairs and certificates on the MX or install them on the MX after enrolling with a certificate authority (CA). The MX can generate key pairs, self-signed certificates, and Certificate Signing Requests (CSRs), as well as install key pairs, server certificates, and certificates generated by a CA.

When the MX communicates with RingMaster, Web View, or an 802.1X or WebAAA client, MSS requests a private key from the MX certificate and key store:

- If no private key is available in the MX certificate and key store, the MX does not respond to the request from MSS. If the MX does have a private key in the key store, MSS requests a corresponding certificate.
- If the MX has a self-signed certificate in the certificate and key store, the MX responds to the request from MSS. If the certificate is not self-signed, the MX looks for a CA certificate to validate the server certificate.
- If the MX has no corresponding CA certificate, the MX does not respond to the request from MSS. If the MX does have a corresponding CA certificate, and the server certificate is validated (date still valid, signature approved), the MX responds.

If the MX does not respond to the request from MSS, authentication fails and access is denied.

For EAP (802.1X) users, the public-private key pairs and digital certificates can be stored on a RADIUS server. In this case, the MX operates as a pass-through authenticator.

## Public Key Infrastructures

A public-key infrastructure (PKI) is a system of digital certificates and certification authorities that verify and authenticate the validity of each party in a transaction through the use of public key cryptography. To have a PKI, the MX requires the following:

- A public key
-

## Public and Private Keys

Trapeze Networks identity-based networking uses public key cryptography to enforce the privacy of data transmitted over the network. Using public-private key pairs, users and devices can send encrypted messages that only the intended receiver can decrypt.

Before exchanging messages, each party in a transaction creates a key pair that includes the public and private keys. The public key encrypts data and verifies digital signatures, and the corresponding private key decrypts data and generates digital signatures. Public keys are freely exchanged as part of digital certificates. Private keys are stored securely.

## Digital Certificates

Digital certificates bind the identity of network users and devices to a public key. Network users must authenticate their identity, and must be able to verify the identity of other users and network devices, such as switches and RADIUS servers.

The Trapeze Networks Mobility System supports the following types of X.509 digital certificates:

- **Administrative certificate**—Used by the MX to authenticate to RingMaster or Web View.
- **MX-MX security certificate**—Used by MX switches in a Mobility Domain to securely exchange management information. (For more information about this option, see the

- **EAP certificate**—Used by the MX to authenticate to (e)-4dc 2gsb3.1988 uthq-6(authAation )Tj[(—Us60 T

# Certificates Automatically Generated by MSS

In cases where certificates are not already configured or installed, and it is the first time an MX is booted with MSS Version 4.2 or later, MSS automatically generates keys and self-signed certificates. MSS can automatically generate all the following types of certificates and their keys:

- 

- **Certificate Signing Request (CSR)**—The most secure method, because the public and private keys for the MX are created on the MX, while the certificate comes from a trusted source (CA). This method requires generating the key pair, creating a CSR and sending it to the CA, cutting and pasting the certificate signed by the CA into the CLI, and then cutting and pasting the CA certificate into the CLI.

**Table D– 2** lists the steps required for each method and refers you to appropriate instructions. (For complete examples, see **"Key and Certificate Configuration Scenarios" on page D–8**.)

**Table D– 2. Procedures for Creating and Validating Certificates**

| Certificate Installation Method | Steps Required | Instructions |
|---|---|---|
| **Self-signed certificate** | 1. Generate a public-private key pair on the MX.<br>2. Generate a self-signed certificate on the MX. | ❑ **"Creating Public-Private Key Pairs" on page D–5**<br>❑ **"Generating Self-Signed Certificates" on page D–6** |
| **PKCS #12 object file certificate** | 1. Copy a PKCS #12 object file (public-private key | |

## Creating Public-Private Key Pairs

To use a self-signed certificate or Certificate Signing Request (CSR) certificate for MX authentication, you must generate a public-private key pair.

To create a public-private key pair, use the following command:

```
crypto generate key {admin | domain | eap | ssh | web}
        {128 | 512 | 1024 | 2048}
```

Choose the key length based on your need for security or to conform with your organizational practices. For example, the following command generates an administrative key pair of 1024 bits:

```
MX# crypto generate key admin 1024
admin key pair generated
```

Some key lengths apply only to specific key types. For example, **128** applies only to **domain** keys.

SSH requires an SSH authentication key, but MSS can automatically generate it. 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.

## Generating Self-Signed Certificates

After creating a public-private key pair, you can generate a self-signed certificate. To generate a self-signed certificate, use the following command:

```
crypto generate self-signed {admin | eap | web}
```

When you type the command, you are prompted to enter information to identify the certificate. For example:

```
MX# crypto generate self-signed admin
Country Name:  S
State Name: CA
Locality Name: San Jose campus
Organizational Name: trapeze.networks
Organizational  nit: eng
Common Name: MX1
Email Address: admin@example.com
 nstructured Name: MX in wiring closet 120
success: self-signed cert for admin generated
```

You include a common name (string) when you generate a self-signed certificate. The other information is optional. Use a fully qualified name if supported on your network. The certificate appears after entering this information.


## Installing a Key Pair and Certificate from a PKCS #12 Object File

PKCS object files provide a file format for storing and transferring storing data and cryptographic information. (For more information, see **"PKCS #7, PKCS #10, and PKCS #12 Object Files" on page D–3**.) A PKCS #12 object file, that you obtain from a CA, includes the private key, a certificate, and optionally the CA certificate.

After transferring the PKCS #12 file from the CA via FTP and generating a one-time password to unlock it, store the file in the MX certificate and key store. To set and store a PKCS #12 object file, follow these steps:

1. Copy the PKCS #12 object file to nonvolatile storage on the MX. Use the following command:

```
copy tftp://filename local-filename
```

2. Enter a one-time password to unlock the PKCS #12 object file. The password must be the same as the password protecting the PKCS #12 file.

   The password must contain at least 1 alphanumeric character, with no spaces, and must not include the following characters:

- Quotation marks ( )
- Question mark (?)
- Ampersand (&)

To enter the one-time password, use the following command:

```
crypto otp {admin | eap | web} one-time-password
```

3.

## Displaying Certificate and Key Information

Follow these steps:

1. Set time and date parameters, if not already set. (See **"Configuring and Managing Time Parameters" on page 8–14**.)
2. Generate public-private key pairs:

```
MX# crypto generate key admin 1024
key pair generated
MX# crypto generate key eap 1024
key pair generated
MX# crypto generate key web 1024
key pair generated
```

3. Generate self-signed certificates:

```
MX# crypto generate self-signed admin
Country Name:  S
State Name: CA
Locality Name: San Francisco
Organizational Name: trapeze.networks
Organizational  nit: I
Common Name: MX 6
Email Address: admin@example.com
 nstructured Name: MX in wiring closet 4
success: self-signed cert for admin generated
MX# crypto generate self-signed eap
Country Name:  S
State Name: CA
Locality Name: San Francisco
Organizational Name: trapeze.networks
Organizational  nit: I
Common Name: MX 6
Email Address: admin@example.com
 nstructured Name: MX in wiring closet 4
Self-signed cert for eap is
success: self-signed cert for eap generated
20# crypto generate self-signed web
Country Name:  S
State Name: CA
Locality Name: San Francisco
Organizational Name: trapeze.networks
Organizational  nit: I
Common Name: MX 6
Email Address: admin@example.com
 nstructured Name: MX in wiring closet 4
success: self-signed cert for web generated
```

4. Display certificate information for verification:

```
MX# show crypto certificate admin
Certificate:
  Version: 3
  Serial Number:  999 (0x3e7)
  Subject: C= S, S =CA, L=PLEAS, O= RPZ, O =SQA, CN=BOBADMIN/emailAddress=BOBADMIN,
         unstructuredName=BOB
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C= S, S =CA, L=PLEAS, O= RPZ, O =SQA, CN=BOBADMIN/emailAddress=BOBADMIN,
         unstructuredName=BOB
  Validity:
```

```
    Issuer: C= S, S =CA, L=PLEAS, O= RPZ, O =SQA, CN=BOBADMIN/emailAddress=BOBADMIN,
           unstructuredName=BOB
    Validity:
        Not Before: Oct 19 01:59:42 2004 GM
        Not After: Oct 19 01:59:42 2005 GM
MX# show crypto certificate web
Certificate:
    Version: 3
    Serial Number:  999 (0x3e7)
    Subject: C= S, S =CA, L=PLEAS, O= RPZ, O =SQA, CN=BOBADMIN/emailAddress=BOBADMIN,
           unstructuredName=BOB
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C= S, S =CA, L=PLEAS, O= RPZ, O =SQA, CN=BOBADMIN/emailAddress=BOBADMIN,
           unstructuredName=BOB
    Validity:
        Not Before: Oct 19 02:02:02 2004 GM
        Not After: Oct 19 02:02:02 2005 GM
```

## Installing CA-Signed Certificates from PKCS #12 Object Files

This scenario shows how to use PKCS #12 object files to install public-private key pairs, CA-signed certificates, and CA certifies for administrative access, 802.1X (EAP) access, and WebAAA access.

1. Set time and date parameters, if not already set. (See **"Configuring and Managing Time Parameters" on page 8–14**.)
2. Obtain PKCS #12 object files from a certificate authority.
3. Copy the PKCS #12 object files to nonvolatile storage on the MX. Use the following command:

```
copy tftp://filename local-filename
```

For example, to copy PKCS #12 files named 2048admn.p12, 20481x.p12, and 2048web.p12 from the TFTP server at the address 192.

For example:

```
MX# crypto pkcs12 admin 2048admn.p12
 nwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
MX# crypto pkcs12 eap 20481x.p12
 nwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
MX# crypto pkcs12 web 2048web.p12
 nwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
```

## Installing CA-Signed Certificates Using a PKCS #10 Object File (CSR) and a PKCS #7 Object File

This scenario shows how to use CSRs to install public-private key pairs, CA-signed certificates, and CA certifies for administrative access, 802.1X (EAP) access, and WebAAA access.

1. Set time and date parameters, if not already set. (See **"Configuring and Managing Time Parameters" on page 8–14**.)
2. Generate public-private key pairs:

```
MX# crypto generate key admin 1024
key pair generated
MX# crypto generate key eap 1024
key pair generated
MX# crypto generate key web 1024
key pair generated
```

3. Create a CSR (PKCS #10 object file) to request an administrative certificate:

```
MX# crypto generate request admin
Country Name:  S
State Name: CA
Locality Name: Cambria
Organizational Name: example.company
Organizational  nit: eng
```

4. Copy the CSR into the CA application.