Release Notes for Mobility System Software Version 7.3.6.3

Juniper Networks recommends that you familiarize yourself with the Known Behaviors and Issues section in this document before installing Mobility System Software (MSS) Version 7.3. For additional product information, refer to the following manual in addition to these release notes:

- Feature Guide for MSS Version 7.3 and RingMaster Version 7.4

Feedback and Support

- Juniper Networks encourages you to provide feedback about your experiences installing and using the product to the Juniper Networks Technical Assistance Center (JTAC). You can contact the JTAC by telephone, e-mail, or fax. If you have a service contract or are a Juniper Authorized Partner, login to Juniper SafetyNet Online at http://www.juniper.net/customers/support/ for additional help.
- Within the US and Canada, call 1-866-877-9822.
- From locations outside the US and Canada, call +1 925-474-2400.
- In non-emergencies, send email to support@juniper.net

Copyright © 2011, Juniper Networks, Inc.

Product Name Changes

Please note that the former Trapeze products now reflect the Juniper Networks product names. .

Former Trapeze Name	Current Juniper Product Name
MXR-2	WLC2
MX-8	WLC8R
MX-200	WLC200
MX-800	WLC800
MX-2800	WLC2800
MP-522	WLA522
MP-632	WLA632

Informational Note:
MX and WLC are interchangeable as is MP and WLA. This reflects the new product branding as a result of the acquisition of Trapeze Networks by Juniper Networks.

What's New in MSS Version 7.3

MSS Version 7.3 contains the following enhancements:

- Support for the WLA522 — The WLA522 is an Enterprise class 2x2 dual-radio 802.11n AP that provides price-performance benefits.

– These are the features supported by MSS 7.3:

  - Easy installation and provisioning
  - Secure and easy manageability
  - Better overall network throughput performance and RF coverage than previous generation MPs
  - Handle more than 25 active wireless client connections per radio
  - Robust and reliable platform
  - Extensible plugin architecture enabling applications related to the complementary technologies such as VoIP, Location, and Video.
  - Efficient diagnostics and troubleshooting capability

- Support for the WLC800R - The WLC800R is a next-generation wireless controller supporting from 16 to 128 MPs. The WLC800R is a 1U system with 8 Gigabit Ethernet ports (4x 1000Base-T, 4xSFP), and built in redundant power supplies.
- Polycom View Certification including WMM and SVP. The documentation is located at Polycom View Certification documentation.
- Support for Juniper-branded Trapeze Networks products. WLCs and WLAs with Juniper rebranding are supported with this version of MSS.

Copyright © 2011, Juniper Networks, Inc.

Version Compatibility

RingMaster

This version of Mobility System Software (MSS) is intended for use with RingMaster Version 7.4 or higher only.

Minimum MSS Requirements for Upgrade

Table 1 lists the minimum MSS version an WLC must be running when you upgrade to MSS Version 7.3. If your WLC is running an older MSS version, you can use the upgrade path to upgrade the WLC to 7.3.

Table 1: Software Requirements for Upgrade to MSS Version 7.3

Product	Minimum MSS Version Required	Upgrade Path
WLC216R WLC200R	5.x	5.0.15.2 -> 6.0.7.2 ->7.0.x.x->7.1.x.x -> 7.3.x.x
WLC2	5.x	5.0.15.2 -> 6.0.7.2 ->7.0.x.x->7.1.x.x -> 7.3.x.x
WLC8R	5.x	5.0.15.2> 6.0.7.2 ->7.0.x.x->7.1.x.x -> 7.3.x.x
WLC800R	7.3.x	N/A
WLC2800	7.0.3.6	7.0.x.x->7.1.x.x -> 7.3.x.x

Upgrading to MSS Version 7.3

Before you upgrade, see **"Version Compatibility" on page 3**. After you verify that the WLC is running the minimum MSS version required to upgrade to MSS Version 7.3, return to this section.

Preparing the MX for the Upgrade

VLAN IDs higher than 3520

Informational Note: To avoid conflicts with the Juniper internal VLAN numbering scheme, it is strongly advised to use VLAN IDs less then 3520 on WLCs that are upgrading to MSS Version 7.3. Failure to do so may result in lost configuration data.

Informational Note: MSS 7.3 includes changes to the storage location of system debug files. Debug information is now stored in persistent user-accessible storage for retrieval after a system restart.

Informational Note: Mobility Domains and Mixed Versions of MSS
When deploying a mixed version Mobility Domain, VLAN tunnels between WLCs with MSS 7.1 and WLC800Rs with MSS 7.3 are not supported.

Copyright © 2011, Juniper Networks, Inc.

Create a backup of your WLC files before you upgrade the WLC.
Juniper Networks recommends that you make a backup of the WLC, before you install the upgrade. If an error occurs during the upgrade, you can restore your WLC to a previous configuration.

Informational Note: When saving the backup file, MSS copies the file to a temporary location to compare it against an existing file for any errors that may have been introduced during the copying process. After verifying that the file is error-free, MSS deletes the file from the temporary location.

You can use the following command to back up the configuration files:

backup system [**tftp:**/*ip-addr*/] *filename* [**all** | **critical**]

To restore an WLC that is backed up, use the following command:

restore system [**tftp:**/*ip-addr*/] *filename* [**all** | **critical**]

"Upgrade Scenario" on page 5 shows an example of the backup command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the Juniper Mobility System Software User's Guide.

Upgrading an Individual WLC Using the CLI

If you have made configuration changes but have not saved the changes, use the save config command to save the changes, before you backup the WLC.

1. Back up the WLC, using the backup system command.
2. Copy the new system image onto a TFTP server.

   For example, log in to http://www.Junipernetworks.com/support/support_portal_login using a Web browser on your TFTP server and download the image onto the server.
3. Copy the new system image file from the TFTP server into a boot partition in the nonvolatile storage of the WLC. For example,

   ```
   WLC200# copy tftp://10.1.1.107/WLC073421.800 boot1:WLC073421.800
   ```

   You can copy the image file only into the boot partition that was not used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.
4. Set the boot partition to the one with the upgrade image for the next restart.
5. To verify that the new image file is installed, type show boot.
6. Reboot the software.

   To restart a WLC and reboot the software, type the following command:

   ```
   reset system
   ```

 Copyright © 2011, Juniper Networks, Inc.

When you restart the WLC, the WLC boots using the new MSS image. The WLC also sends the WLA version of the new boot image to MPs and restarts the MPs. After an WLA restarts, the version of the new WLA boot image is checked to make sure the version is newer than the version currently installed on the WLA. If the version is newer, the WLA completes installation of the new boot image by copying the boot image into the WLA flash memory, which takes about 30 seconds, then restarts again. The upgrade of the WLA is complete after the second restart.

Upgrade Scenario

To upgrade a WLC800R, use the following upgrade example.

This example copies the image file into boot partition 1. On your WLC, copy the image file into the boot partition that was not used the last time the WLC was restarted. For example, if the WLC booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the show boot command.

```
WLC800R# save config
success: configuration saved.
WLC800R# backup system tftp:/10.1.1.107/sysa_bak
success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
WLC800R# copy tftp://10.1.1.107/WLC073421.800 boot1:WLC073421.800
.....
.....
.....success: received 10266629 bytes in 92.427
seconds [ 111078 bytes/sec]
WLC800R# set boot partition boot1
success: Boot partition set to boot1:WLC073421.800 (7.3.4.2).
WLC800R# show boot
Configured boot version:         7.3.4.2
Configured boot image:           boot1:WLC073421.800
Configured boot configuration:   file:configuration
Backup boot configuration:       file:backup.cfg
Booted version:                  7.3.4.2
Booted image:                    boot1:WLC07333.800
Booted configuration:            file:configuration
Product model:                   WLC
WLC800R# reset system
...... rebooting ......
```

When saving the backup file, MSS copies the file to a temporary location to compare it against an existing file for any errors that may have been introduced during the copying process. After verifying that the file is error-free, MSS deletes the file from the temporary location.

Copyright © 2011, Juniper Networks, Inc.

Installing Upgrade Activation Keys on an WLC

WLA licensing is supported on WLC platforms as shown in **Table 2**:

Table 2: Licensing and Upgrade Increments for the WLC Models

WLC Model	Base WLA Support	Maximum WLA Support	Upgrade Increment
WLC800R	16	128	16
WLC200R/WLC 216R	32	192	32
WLC2800	64	512	64

If you downgrade to a previous version of MSS that does not support the higher capacity licenses, the number of allowed MPs is reduced to comply with the older software limitations.

Feature licensing is supported on WLC platforms as show in **Table 3**.

Table 3: WLC Feature Licensing Matrix

WLC Model	Advance Voice Module	High Availability Module	Mesh/Bridging Module
WLC2	Supported	Not Supported	Up to 4 MPs (16 MPs in Cluster mode)
WLC8R	Supported	Not Supported	Up to 12 MPs (48 in Cluster mode)
WLC800R	Supported	Supported	Up to 128 MPs (512 MPs in Cluster mode)
WLC200R and WLC216R	Supported	Supported	Up to 192 MPs (768 in Cluster mode)
WLC2800	Supported	Supported	Up to 512 MPs (4096 in Cluster mode)

To upgrade an WLC license:

1. Obtain a license coupon for the upgrade from Juniper Networks or your reseller.
2. Establish a management session with the WLC to display the serial number. To display the serial number, type the following command:

   show version

   In the following example, the WLC serial number is 1234567890:

```
WLC> show version

Mobility System Software, Version: 7.3.4.2 REL
        Copyright (c) 2002 - 2011 Juniper Networks, Inc. All rights reserved.

Build Information: (build#0) REL_7_3_1_branch 2008-08-02 14:21:00
Model:             WLC200
Hardware
   Mainboard:      version 24 ; revision 3 ; FPGA version 24
   PoE board:      version 1 ; FPGA version 6
```

 Copyright © 2011, Juniper Networks, Inc.

```
Serial number       1234567890
Flash:              7.3.0.2.0.0.49  - md0a
Kernel:             3.0.0#112: Wed Aug  2 10:26:32 PDT 2009
BootLoader:         7.3 / 7.3.1
```

3. Use a Web browser to access the Juniper Networks license server at the following URL:

   https://www.juniper.net/generate_license/

4. Type your e-mail address in the E-mail and Confirm E-mail fields.
5. Select your WLC model or a feature to upgrade an AP license or a licensed feature from the License Selection list.
6. Type or copy and paste the WLC serial number into the Product Serial Number field, and click OK. The Product Licensing page appears.
7. Type the coupon activation code(s) into the Coupon Code(s) fields and click OK. The Licensing Confirmation page appears, and displays the activation key (also called the license key).
8. Highlight and copy the entire activation key.
9. On the WLC, use the following command at the enable (configuration) level of the CLI to install the activation key:

   set license activation-key

   In the following example, an activation key for an additional 96 MPs is installed on an WLC200:

   ```
   WLC800R# set license 3B02-D821-6C19-CE8B-F20E
   success: license accepted
   ```

10. Verify installation of the new license by typing the following command:

    ```
    WLC800R# show licenses
    Feature           : 96 additional MPs
    ```

    Support for the additional MPs begins immediately. You do not need to restart the WLC to place the upgrade into effect.

System Parameter Support

Table 4, **Table 5**, and **Table 6** list the recommended or maximum supported values for major system parameters.

Table 4: Mobility System Parameters

Parameter	Supported Value
WLC switches in a single Network Domain	500
WLC switches in a single Mobility Domain	64
Roaming VLANs per WLC	• WLC2800: 256 total (256 configured) • WLC800R: 256 total (128 configured) • WLC200R/216R: 256 total (128 configured) • WLC8R: 256 total (128 configured) • WLC2: 256 total (128 configured)
VLANs per Mobility Domain	2048

Copyright © 2011, Juniper Networks, Inc.

Table 4: Mobility System Parameters (continued)

Parameter	Supported Value
MPs per WLC	• WLC2800: 4096 configured, 512 active • WLC800R: 512 configured, 128 active • WLC200R: 768 configured, 192 active • WLC216R: 768 configured, 192 active • WLC8R: 48 configured, 12 active • WLC2: 16 configured, 4 active Includes directly attached MPs and Distributed MPs. Inactive configurations are backups.
Minimum link speed between WLCs in a Mobility Domain	128 Kbps
Minimum link speed between an WLC and AP in a Mobility Domain	128 Kbps and 95ms round trip latency
Number of Service Profiles per WLC	• WLC2: 32 • WLC8R: 32 • WLC200R: 192 • WLC216R: 192 • WLC800R: 128 • WLC2800: 512
Number of Radio Profiles per WLC	• WLC2: 4 • WLC8R: 12 • WLC200R: 192 • WLC216R: 192 • WLC800R: 128 • WLC2800: 512

Table 5: Network Parameters

Parameter	Supported Value
Forwarding database entries	• WLC2800: 32768 • WLC800R: 32768 • WLC200R: 8192 • WLC216R: 8192 • WLC8R: 8192 • WLC2: 8192
Statically configured VLANs	• WLC2800: 512 configured • WLC800R: 256 configured • WLC200R/216R: 128 configured • WLC8R: 128 configured • WLC2: 128 configured
Spanning trees (STP/PVST+ instances)	64

Copyright © 2011, Juniper Networks, Inc.

Table 5: Network Parameters (continued)

Parameter	Supported Value
ACLs	ACEs per WLC • 170 ACEs per ACL: • WLC2800: 256 • WLC800R: 256 • WLC200R: 256 • WLC216R: 256 • WLC8R: 25 • WLC2: 25
Location Policies	Location Policies per WLC: All models: 1 The Location Policy can have up to 150 rules.
IGMP streams	500 **Note:** Replication of a stream on multiple VLANs counts as a separate stream on each VLAN.
Mesh Services and Bridging	• Mesh Depth — 3 Mesh Links (Portal<->Mesh WLA<->Mesh WLA) • Mesh Fan Out— 6 WLAs • Maximum Supported Mesh Nodes per Mesh Portal — 6 • Bridge Links — 1:1:1

Table 6: Management Parameters

Parameter	Supported Value
Maximum instances of RingMaster simultaneously managing a network	3
Telnet management sessions	• WLC2800: 8 • WLC800R: 8 • WLC200R: 8 • WLC216R: 8 • WLC8R: 4 • WLC2: 4 The maximum combined number of management sessions for Telnet and SSH together is 8 for the WLC400, WLC200, and WLC216, or 4 for the WLC8R and WLC2, in any combination.

Copyright © 2011, Juniper Networks, Inc.

Table 6: Management Parameters (continued)

Parameter	Supported Value
SSHv2 management sessions	• WLC2800: 8 • WLC800R: 8 • WLC200R: 8 • WLC216R: 8 • WLC8R: 4 • WLC2: 4
Telnet client sessions (client for remote login)	• WLC2800: 8 • WLC800R: 8 • WLC200R: 8 • WLC216R: 8 • WLC8R: 4 • WLC2: 4
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS and LDAP servers	40 configured on the WLC 4 in a server group 4 server groups in a AAA rule A maximum of 40 servers in any combination of RADIUS and LDAP - for example, 30 RADIUS servers and 10 LDAP servers.

Table 7: Client and Session Parameters

Parameter	Supported Value
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total.
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data.

Copyright © 2011, Juniper Networks, Inc.

Table 7: Client and Session Parameters (continued)

Parameter	Supported Value
Active AAA sessions (or clients trying to establish active connections) per WLC	• WLC2800: 12800 • WLC800R: 3200 • WLC200R: 4800 • WLC216R: 4800 • WLC8R: 300 • WLC2: 100
AAA users configured in local database	• WLC2800: 1000 • WLC800R: 1000 • WLC200R: 1000 • WLC216R: 1000 • WLC8R: 250 • WLC2: 250

Known Behaviors and Issues

The following issues are known behaviors and issues in this version of Mobility System Software.

- If an WLA has vlan-tagging enabled, it does not boot in bridging mode. (61935)

  Description — The static VLAN tag is not supported in mesh and bridging modes. It is not a valid configuration to enable both at the same time.

  Workaround— N/A.

Issues Resolved Since Version 7.3.5.2

- The WLC800R was blocking any IPv6 connectivity. (66653)
- A WLA was deauthenticating clients for no specific reason which caused connectivity issues for VoIP phones. (66221), [PR656147]
- Deleting a Mobility Domain did not propagate the changes to RingMaster which incorrectly reported the configuration. (67373), [PR657287]
- Occasional radar detection by an outdoor Mesh network setup caused connection issues on the bridge link. (67396), [PR657310]
- On the WLC800R, clients attempting a connection to an encrypted SSID, and Port Group was configured, did not connect successfully. (68313), [PR658220]
- Disabling l2-restrict did not work as expected. The only way to disable the feature was to remove the rule using the CLI. (68437), [PR658338]
- After upgrading to MSS 7.3.5.2, certain VoIP handsets did not operate properly. (68439), [PR658340]
- ASCOM handsets did not work correctly when roaming from WLA to WLA. (68461), [PR658361]

Issues Resolved Since Version 7.3.4.4

- After a WLC tunnel moved to a dormant state, the tunnel could not become active again. (67695)

Copyright © 2011, Juniper Networks, Inc.

- A Linux client with a iwlagn driver did not correctly negotiate the MCS rates when reconnecting to the network. (67820)
- For MAC clients, Bonjour stopped working on the network. (67744)
- When using the Web Portal feature, the admin certificate was sent out instead of the web-portal certificate. (67709)
- It appeared that Mac clients were bypassing bonded authentication on an SSID if they successfully connected to another SSID. (67653)
- With no-broadcast enabled, Windows Vista clients sent out DHCP DISCOVERS as a broadcast with a broadcast flag set, and could not obtain IP addresses on the network. (67544)
- After upgrading the MSS, APs did not appear in the `show ap status` output. (67399)
- The auto-tune feature in MSS stopped working correctly. (67303)
- Client authorization failed to work correctly if the Web Portal client attempted to reconnect to the same AP. (67101)
- The noise floor attribute did not fluctuate for some AP models.(67073)
- There were a large number of 802.11 retries on the network which affected VoIP quality. (67000)
- Some AP LEDs were blinking amber and incorrectly indicating the status of the AP. (66763)
- RF detect counters were not incrementing correctly for management types 6, 7, d, e, and f flood attacks. (66750)
- The timezone on an WLC was not configured correctly using the quickstart wizard. (66630)
- The AP affinity feature was not working correctly. The PAM and SAM were selected from the same group of WLCs. (66493)
- Users could not connect to a wireless network if the remote AP was connected to a WLC configured with NAT. (66362)

Issues Resolved Since Version 7.3.4.4

- Using the command **`show AP status all`** did not display all of the APs on the network. (66308)
- The SIP-aware feature was not working as expected. (66294)
- When using WebPortal Local Switching on a network with WLA82s, clients repeatedly connected and disconnected on the network. (66270)
- When command auditing is enabled on the WLC, the log file became too large and you could not upgrade to new MSS versions. (66266, 66050)
- Under heavy client load, the WLC incorrectly classified APs as rogues and BSSID spoofs. (65203)
- A high CCMP decryption error count appeared on Mesh APs in a fanout installation. (65015)
- Web-portal did not work if it is disabled and then re-enabled. (62547)
- Using the command, **show fdb all port**, did not display port lists. (62242)
- Some cluster configuration changes on the WLC were not accurately reflected by RingMaster.(59864)

 Copyright © 2011, Juniper Networks, Inc.

Issues Resolved Since Version 7.3.2.3

- Session monitoring did not collect the same information as it did in a previous version of MSS which impacted session monitoring in RingMaster. (65568)
- An empty certificate file prevented the WLC200 from performing the boot process.(65483)
- The WLC was attempting to obtain an IP address from the wrong DNS server. (65047)
- The WLA radio was falsely reporting jamming detection on the network. (64822)
- Trace logs for 802.1X clients did not contain the proper information. (63934)

Issues Resolved Since Version 7.3.0.3

- Association with an WLA was successful but then WLA disconnected the session. (65269)
- IP addresses were not matching correctly on corresponding ACLs. (65146)
- The WLC800 was reporting "Failed Fans" status during beta tesing. (64798, 64192)
- The ability to schedule a command for execution on the WLC such as 'redirect' was not implemented in MSS. (64797)
- Increases in the No Receive Descriptor and Radio Reset counters caused problems for VoIP clients on the network. (64474)
- Throughput on the WLA82 was not as expected in previous releases. (64320)
- Intel 5100/5300 11n client did not connect consistently with the WLA82. (64291)
- Mesh APs were timing out on the network. (64302)
- The WLA620 was inaccurately reporting DFS channel scans. (64174)
- The time on the WLC was drifting from the actual time on the network. (64806, 64156)
- A large number of error messages appeared on the network when an WLA roamed from one WLC to another. (63914)
- When upgrading from an earlier version of MSS, CA certificates were deleted from the configuration. (63866)
- Some SSIDs were erroneously classified as rogue SSIDs on the network. (63829)
- The system timestamp was incorrectly reporting the time due to NTP issues. (64806)
- Configuring port groups did not work after upgrading from 7.1 to 7.3.(63641)
- Some APs did not upgrade correctly due to bootcode errors. (63652)
- Having multiple versions of MSS in a cluster configuration caused the configuration to become unresponsive on the network. (63577)
- MSS displayed the incorrect timestamp in logfiles. (63306)
- Some clients could not connect to MPs on the network. (63272)
- When the command "show fdb all port ?" was used, you were prompted for a list of ports. However, if you attempted to enter a list of ports, MSS returned the error, "invalid port". (62242)
- Configuring a filter for network traces did not filter the traces. (63095)

Copyright © 2011, Juniper Networks, Inc.

Documentation Errata

- Indoor Mobility Point Quick Installation Guide

– The installation instructions mention using two RJ-45 cables on the WLA522 for redundancy. However, the WLA522 only has one port and can use only one cable.

- WebView

– The MSS Quick Start Guide is missing information about logging into WebView. (65947)

– To log into WebView, you need a username and password. The default username is admin and the default password is no password. Follow these steps to log into WebView:

1. In a Web browser, type the IP address of the WLC using the format, https://<ipaddress>.

2. In the Username field, type admin.

3. If you have not configured an enable password for the WLC, leave the Password field blank and click OK. If you have configured an enable password for the WLC, type that in the Password field.

- Web Portal

Web authentication over IPv6 is not supported by MSS, but IPv6 clients can be blocked by adding an ACE to deny IPv6 to the web-portal ACL (ARP must be permitted).

```
WLC# set security acl name portalacl permit mac 00:00:00:00:00:00
     ff:ff:ff:ff:ff:ff 00:00:00:00:00:00 ff:ff:ff:ff:ff:ff ethertype 806
WLC# set security acl name portalacl deny mac 00:00:00:00:00:00
     ff:ff:ff:ff:ff:ff 00:00:00:00:00:00ff:ff:ff:ff:ff:ff ethertype 86dd
WLC# set security acl name portalacl permit udp 0.0.0.0 255.255.255.255 eq 68
     0.0.0.0 255.255.255.255 eq 67
WLC# set security acl name portalacl deny 0.0.0.0 255.255.255.255 capture
     commit security acl portalacl
```

- In the MSS Configuration Guide, on page 24-21 under `restricting client-to-client forwarding among IP-only clients`, the incorrect syntax in step 6. It currently reads as follows: (61453)

```
WLC# set security acl name c2c map vlan vlan-1 out
WLC# set security acl name c2c map vlan vlan-1 in
```

  The correct syntax should be

```
WLC# set security acl name map c2c vlan vlan-1 out
WLC# set security acl name map c2c vlan vlan-1 in
```

- The ACL edit buffer is meant to be used for creating and editing one ACL at a time. If you need to create multiple ACLs, use 'commit security acl all' after each ACL. This is not fully documented in the MSS User's Guide. (61703)
- An RF detect blacklist is applied across Mobility Domains. This is not stated in the MSS Configuration Guide. (65905)
- Starting with 7.0, the dot1x reauth-period works only on a dynamic WEP and WPA with WEP-40 or WEP-104 cipher. In case that both the dot1x reauth-period and session-timeout attribute (from the service profile or RADIUS) are set, the session-timeout attribute value is used.
- The WPA with TKIP or CCMP cipher uses only the session-timeout attribute from service profile or RADIUS, if set. (61158)

 Copyright © 2011, Juniper Networks, Inc.

- It is not stated clearly in the MSS Configuration Guide that Network Address Translation (NAT) is not supported in a cluster configuration. (57596)
- The MIB, trpzApState, is not documented in the MSS Command Reference or MSS Configuration Guide. SNMP queries on 'trpzApStatApStatusApState' or 'trpzApStatApStatusMacApState' on an MX acting as SAM for an AP in cluster will return the value '0' for that AP. This value is the equivalent of 'redundant' in CLI, which means that the link between that AP and the MX is for backup. [PR673913]

Miscellaneous Issues including Changes to Default Behaviors

- The cipher-wep40 and cipher-wep104 service-profile options are deprecated due to Wi-Fi certification requirements. (65065, 64259)
- Evaluation Licensing Behavior — The evaluation license does not replace any existing feature licenses. If there are feature licenses installed, then the existing feature licenses take precedence over the evaluation license. In this case, the evaluation license fills in the gaps for existing licenses. (63950)
- Auto-tune channel-config lockdown feature does not work in cluster mode. When operating in Cluster mode, the auto-tune channel lockdown command is not available. Auto-tune lockdown must be completed via alternate mechanisms. e.g. RingMaster or auto-tune lockdown while in a basic Mobility Domain configuration. (66307, 62746)

© 2011 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, the Mobility System, Mobility Exchange, MX, Mobility Point, MP, Mobility System Software, MSS, RingMaster, AAA Integration and RADIUS Scaling, ActiveScan, AIRS, Bonded Auth, FastRoaming, Granular Transmit Power Setting, GTPS, GuestPass, GuestTunneling, Layer 3 Path Preservation, Location Policy Rule, LPR, Mobility Domain, Mobility Profile, Passport-Free Roaming, SentryScan, Time-of-Day Access, TDA, TAPA, Trapeze Access Point Access Protocol, Virtual Private Group, VPG, Virtual Service Set, Virtual Site Survey, Wireless Access Routing Protocol, WARP and WebAAA are trademarks of Juniper Networks, Inc. All other products and services are trademarks, registered trademarks, service marks or registered service marks of their respective owners.

Copyright © 2011, Juniper Networks, Inc.