WLM1200-RMTS™ User's Guide

WLM1200-RMTS™ User Guide

Contents

WLM1200-RMTS Publication Suite

This guide is part of a publications suite that describes the *WLM1200-RMTS* installation and operation. It is intended for network administrators or persons responsible for installing and using a *WLM1200-RMTS* for managing 802.11-based Wireless LANs (WLANs) using Juniper hardware and software.

The following documents provide information on how to plan, install, configure and manage a *WLM1200-RMTS*.

- WLM1200-RMTS Hardware Setup Guide — Provides procedures for site preparation, physical installation and cabling connections.
- WLM1200-RMTS Quick Start — This guide provides a description of prerequisite procedures required to install and begin using RingMaster Appliance hardware and software.
- WLM1200-RMTS User's Guide (this document) — This guide describes the Juniper Networks WLM1200-RMTS Appliance, which delivers the RingMaster application combined with an Operating system (OS) on an appliance hardware platform. This appliance eliminates setting up of an execution environment for a RingMaster Server. By providing an execution environment, this appliance delivers an assured level of scalability, along with reduced maintenance overhead. After performing basic configuration to incorporate the appliance into a network, normal maintenance involves installation of periodic updates from Juniper Networks.

WLM1200-RMTS Hardware Description

The WLM1200-RMTS Appliance is a platform is a server on which to run *RingMaster Services* software. This device has the hardware features, *OS* and *RingMaster* software required to function as a server for RingMaster Software.

Processors and RAM

- Two Quad-Core Intel Xeon 2.66 GHz CPUs
- 4 GB RAM

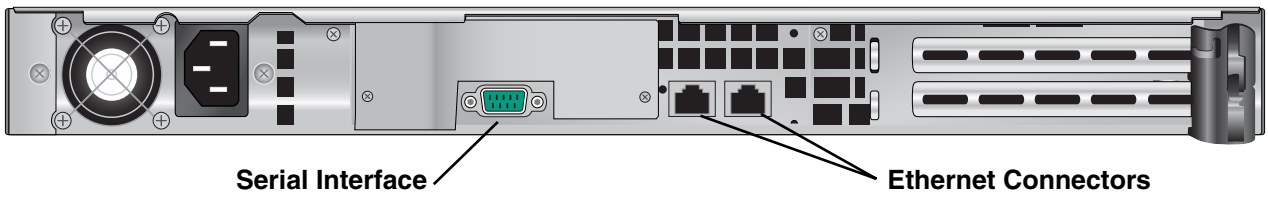
Disk Configuration

- Two 250 GB Hard Drives

Hardware Description

WLM1200-RMTS is set up with a dual boot partition scheme. One partition holds the active (running) system image and the other partition holds the standby (next) system image. An interface provides for management of these partitions. In order to provide reliability in the case of a disk failure, the system utilizes disks in a RAID-1 mirroring scheme.

Interfaces



- Serial console port
- Two 10/100/1000 Base T interfaces

Software Description

OS

The *RingMaster* appliance runs on the *Linux* operating system. The WLM1200-RMTS does not provide any means of accessing the OS shell to run arbitrary commands.

CLI

A Command Line Interface (CLI) is provided through a serial port. This interface allows configuration of platform-related settings and is equivalent to that of the platform configuration Web interface. The CLI provides a subset of the functionality provided by the Web interface. For details, see Using The Command Line Interface below.

Web

The WLM1200-RMTS supports a Web interface for configuring RingMaster tunables plus a new interface for configuring platform-related settings like networking, date/time, etc. The RingMaster configuration Web interface is accessed via HTTPS on port 443. You have the option as to whether or not access control should be enabled for this interface. The WLM1200-RMTS's platform configuration Web interface is accessed via HTTPS on port 8003. Links in both interfaces allow navigation between the two. Access control is always enabled for the platform configuration Web interface. There are two users — admin and monitor — defined for the platform settings Web interface.

Image Upgrade

WLM1200-RMTS software is distributed as a single image containing both the *OS* and the *RingMaster* application. The installation procedure is based on an active/standby partitioning scheme where the new software is setup in the standby partition. The system does not reboot itself as part of an upgrade. The upgrade sets up the standby partition. You must make upgrades effective by manually rebooting the system. If anything goes wrong during an installation procedure, the system resorts to running the previously active partition.

A Web-based mechanism is also provided for you to manually revert to the previously active partition at any time. If this revert operation is invoked, the state of the *RingMaster* application (plans and monitoring database) also reverts to the state at which the previous installation occurred.

Factory Reset

The WLM1200-RMTS supports a CLI-based mechanism to reset the platform and *RingMaster* application settings back to default settings. This operation does not affect the executable software running on the appliance. It resets the configuration to a default state compatible with currently active software. Any existing *RingMaster* plans as well as the monitoring database are cleared as part of this operation. All licensing information is also deleted.

A mechanism is provided to reset the **admin** password should you forget it. This mechanism is only provided through the CLI on the serial port. The reset operation does not affect any other platform configuration other than the password.

Licensing

License Distribution

The WLM1200-RMTS is shipped with a license certificate for 250 APs. You must install and activate the base license and all additional AP licenses.

Appliance Installation

Complete instructions regarding site preparation, unit unpacking and equipment installation are provided in the publication *WLM1200-RMTS Hardware Setup Guide* including information on cabling connections to the unit from a power source and for networking interfaces.

Platform Configuration

Initial RingMaster Setup

When the WLM1200-RMTS is shipped, *RingMaster* software is already installed, including the latest OS and *RingMaster* software. When powering up for the first time, the only function available to you is the setup wizard. You use this initial setup wizard to specify basic platform information, such as how to connect to a network, before appliance functionality is enabled. This wizard is implemented as a CLI-based mechanism accessible through the appliance's serial port.

When you connect to this port, you are prompted for the following information:

- Hostname
- Networking
  - Selection of DHCP or static IP
  - If static IP
    - IP address and netmask
    - Default gateway
    - IP address of primary name server and domain name
- Administrator password — The wizard uses this to set up a user named **admin**.

Command Line Interface

A command line interface is supported on the appliance's serial port. The commands supported provide a subset of the functionality provided by the Web interface.

Specifically, the following is supported:

- Networking
- Image Upgrade
- Factory Reset
- Shutdown/Reboot

The one CLI-only function is the factory reset command.

Using The Command Line Interface

The CLI presents a prompt with the platform name, which in our example above is **rm200a1**.

This prompt looks like this:

```
rm200a1 >
```

When in enabled mode, this prompt changes to the following:

```
rm200a1 #
```

CLI Commands

The CLI for this device includes a number of commands, as listed below from capture from an WLM1200-RMTS, showing commands implemented and options for accessing them and getting help regarding their use.

Login

```
login as: admin

Trapeze Networks WLM1200-RMTS Platform
Last login: Mon Dec 10 22:33:34 2007 from 172.21.26.220

Trapeze Networks WLM1200-RMTS Platform
```

Getting Help

```
rm200a1 # help ?
<cr>
rm200a1 # help
You may request context-sensitive help at any time by pressing '?'
on the command line.  This will show a list of choices for the
word you are on, or a list of top-level commands if you have not
typed anything yet.
```

If "<cr>" is shown, that means that what you have entered so far s a complete command, and you may press Enter (carriage return) to execute it.

Try the following to get started:

```
?
show ?
show c?
show clock?
show clock ?
show interfaces ?     (from enable mode)
```

show ? Command

```
rm200a1 > show ?

bootvarDisplay installed system images and boot parameters
hostsDisplay hostname, DNS configuration, and static host mappings
imagesDisplay information about system images and boot parameters
terminalDisplay terminal parameters
versionDisplay version information for current system image
whoamiDisplay the identity and capabilities of the current user
```

show bootvar Command

```
rm200a1 > show bootvar

Installed images:
  Partition 1:
  ringmaster 6.3.1.0.3 #1-dev 2007-12-10 08:25:40 i386 root@rmabuild:unknown

  Partition 2:
  ringmaster 6.3.0.0.51 #1-dev 2007-11-27 09:57:16 i386 root@rmbuild:cvs/HEAD

Last boot partition: 1
Next boot partition: 1

No boot manager password is set
```

show hosts Command

```
rm200a1 > show hosts

Hostname: rm200a1
Name server: 172.21.129.10 (dynamic)
Name server: 172.21.129.33 (dynamic)
Domain name: trpz.com (dynamic)
IP 127.0.0.1 maps to hostname localhost
IP 127.0.0.1 maps to hostname rm200a1
```

show terminal Command

```
rm200a1 > show terminal

CLI current session settings
  Terminal width:           80 columns
  Terminal length:          24 rows
  Terminal type:            xterm
```

show version Command

```
rm200a1 > show version

Product name:      ringmaster
Product release:   6.3.1.0.3
Build ID:          #1-dev
Build date:        2007-12-10 08:25:40
Build arch:        i386
Built by:          root@rmabuild.trpz.com

Uptime:            46m 5.780s

Product model:     rm200
Host ID:           07f98f2901db
System memory:     284 MB used / 3609 MB free / 4041 MB total
Number of CPUs:    8
CPU load averages: 0.01 / 0.03 / 0.00
```

show whoami Command

```
rm200a1 > show whoami

Current user: admin
```

```
rm200a1 > en
rm200a1 # show ?
bootvar          Display installed system images and boot parameters
hosts            Display hostname, DNS configuration, and static host mappings
images           Display information about system images and boot parameters
interfaces       Display detailed running state for all interfaces
ip               Display IP-related information
log              View event logs
running-config   Display commands to recreate current running configuration
terminal         Display terminal parameters
version          Display version information for current system image
whoami           Display the identity and capabilities of the current user
```

Enable Mode

After you type enable or en at a `rm200a1 >` prompt, you see a `rm200a1 #` prompt:

Enable Mode Commands

```
rm200a1 # ?
configure        Enter configuration mode
disable          Leave enable mode
email            Configure email and event notification via email
exit             Log out of the CLI
help             View description of the interactive help system
image            Manipulate system software images
no               Negate or clear certain configuration options
ping             Send ICMP echo requests to a specified host
reload           Reboot or shut down the system
show             Display system configuration or statistics
terminal         Set terminal parameters
write            Save the running configuration to persistent storage
```

configure ? Command

```
rm200a1 # configure ?
terminal         Enter configuration mode
```

show clock Command

```
rm200a1 # show clock
Time: 23:30:21
Date: 2007/12/10
Time zone: GMT-offset GMT
```

configure terminal Command

```
rm200a1 # configure terminal

rm200a1 (config) # show ?
bootvar          Display installed system images and boot parameters
hosts            Display hostname, DNS configuration, and static host mappings
images           Display information about system images and boot parameters
interfaces       Display detailed running state for all interfaces
ip               Display IP-related information
log              View event logs
running-config   Display commands to recreate current running configuration
terminal         Display terminal parameters
version          Display version information for current system image
whoami           Display the identity and capabilities of the current user
rm200a1 # email ?
send-test        Send test email to all configured event and failure recipients
```


show image Command

```
rm200a1 # show image
Images available to be installed:
  webimage.tbz
  ringmaster 6.3.1.0.3 #1-dev 2007-12-10 08:25:40 i386 root@rmabuild:unknown

Installed images:
  Partition 1:
  ringmaster 6.3.1.0.3 #1-dev 2007-12-10 08:25:40 i386 root@rmabuild:unknown

  Partition 2:
  ringmaster 6.3.0.0.51 #1-dev 2007-11-27 09:57:16 i386 root@rmbuild:cvs/HEAD

Last boot partition: 1
Next boot partition: 1

No boot manager password is set.
```

ping Command

```
rm200a1 # ping
Usage: ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
            [-M mtu discovery hint] [-S sndbuf]show ?
Show ?
?
            [ -T timestamp option ] [ -Q tos ] [hop1 ...] destination
```

show ip ? Command

```
rm200a1 # show ip ?
default-gateway  Display the active default route
route            Display routing table

rm200a1 # show running-config
##
## Running database "initial"
##

##
## Network interface configuration
##
   interface eth0 create
   interface eth0 dhcp
   interface eth0 display
   interface eth0 duplex auto
   interface eth0 mtu 1500
no interface eth0 shutdown
   interface eth0 speed auto
no interface eth0 zeroconf

##
## Other IP configuration
##
   ip host rm200a1 127.0.0.1
   hostname rm200a1
```

show terminal Command

```
rm200a1 # show terminal
CLI current session settings
  Terminal width:           80 columns
```

```
  Terminal length:          24 rows
  Terminal type:            xterm
```

show version Command

```
rm200a1 # show version
Product name:      ringmaster
Product release:   6.3.1.0.3
Build ID:          #1-dev
Build date:        2007-12-10 08:25:40
Build arch:        i386
Built by:          root@rmabuild.trpz.com

Uptime:            58m 7.760s

Product model:     rm200
Host ID:           07f98f2901db
System memory:     285 MB used / 3606 MB free / 4041 MB total
Number of CPUs:    8
CPU load averages: 0.00 / 0.00 / 0.00
```

Forgotten Password Recovery

If the administrator of a system forgets the password of the user **admin**, the following method can be used to reset the password to the empty password so that the system can be accessed as **admin** with no password required. The password can then reset to a secure one via the CLI.

The procedure is as follows:

1. Boot the system to single user and execute a script to reset the **admin** password in the active database. If any database corruption is suspected, the script resets the system database to its initialized default. The **admin** password is not set in such a database. A system booted to single user mode does not require a privileged user password. The system can be rebooted by power cycling. It is assumed the person using this procedure is able to access the system's console and can see the entire boot process (this is either over a serial console or the system's direct console).
2. Once the system is starting to boot, the following GRUB message should be seen (GRUB is the boot loader for the system):

   ```
   Grub Loading stage 2...
   Press any key to continue.
   ```

   [This message repeats (once a second) on a new line several times, and if no key is pressed the system boots normally. You should press a key to enter the GRUB command line]

   ```
   .
   .
   .
    Press any key to continue.
   ```

   [Assume the user presses the space key (for example)]
3. Next, you should see the following GRUB text which allows you to select one of the 2 images to be booted. Choose the desired image by using the arrow keys so that GRUB indicates that the desired entry will be booted.

   ```
       GRUB  version 0.93  (640K lower / 259536K upper memory)

   ------------------------------------------------------------------------
   ```

```
 0: genericamp/linux demo #1-dev 2004-02-29 23:16:14
      root@saturn5:CVS_TMS/HEAD
 1: genericamp/linux demo #1-dev 2004-02-29 23:16:14
      root@saturn5:CVS_TMS/HEAD
-----------------------------------------------------------------

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, 'e' to edit the
      commands before booting, 'a' to modify the kernel arguments
      before booting, or 'c' for a command-line.

    Highlighted entry is 1:
```

If a selection is not made within a few seconds, the system will automatically boot the image that is highlighted. You should press the **e** key to enter the edit command mode. This will give you the ability to change command options that are part of the boot process. Specifically, you will add the option **single** to force the system into single user mode.

When the **e** key is pressed, the GRUB text shown below will be seen. (Note the **0** and **1** entries now refer to the selected image that is booting). You should now edit the **kernel** line. This is done using the arrow keys on your keyboard to select the **1:** line — press the down arrow key one time. The message at the bottom should now indicate **Highlighted entry is 1:**

```
    GRUB  version 0.93  (640K lower / 259536K upper memory)

-----------------------------------------------------------------
 0: root (hd0,1)
 1: kernel /vmlinuz ro root=/dev/hda5 console=tty0 console=ttyS0,9600n8
-----------------------------------------------------------------

      Use the ^ and v keys to select which entry is highlighted.
      Press 'b' to boot, 'e' to edit the selected command in the
      boot sequence, 'c' for a command-line, 'o' to open a new line
      after ('O' for before) the selected line, 'd' to remove the
      selected line, or escape to go back to the main menu.

    Highlighted entry is 1:
```

4. After selecting the **1: kernel** command line, press the **e** key to edit this line.
5. After **e** is pressed, you should see the **grub edit>** prompt. If the line is long enough, you may only see a portion of the end of the text. For example, in the above when the **1: kernel** line is:

   ```
   kernel /vmlinuz ro root=/dev/hda5 console=tty0 console=ttyS0,9600n8
   ```

   after 'e' is pressed, the user may see the following

   ```
   <yS0,9600n8
   ```

   The **<** indicates the a portion of the command line is not seen. The arrow keys allow you to navigate the command line.

   The option **single** should be appended to the end of this line. For example:

   ```
     <yS0,9600n8 single

       GRUB  version 0.93  (640K lower / 259536K upper memory)

   -----------------------------------------------------------------
    0: root (hd0,1)
    1: kernel /vmlinuz ro root=/dev/hda5 console=tty0 console=ttyS0,9600n8 sin-
         gle
   ```

```
----------------------------------------------------------------------

      Use the ^ and v keys to select which entry is highlighted.
      Press 'b' to boot, 'e' to edit the selected command in the
      boot sequence, 'c' for a command-line, 'o' to open a new line
      after ('O' for before) the selected line, 'd' to remove the
      selected line, or escape to go back to the main menu.

   Highlighted entry is 1:
```

It should be noted that two 'console' options appear on the **kernel** line. In this example, the latter is the serial console and the former is the direct console. The **console** option that appears last is used. If the procedure is used on the direct console, the order of the two **console** options should be changed or the serial one (console=ttyS0,9600n8) should be deleted.

6. When done editing the **kernel** line, press the <enter> key followed by the **b** key to resume booting the selected image. After more boot messages a **root** user prompt will be displayed:

```
sh-2.05b#
```

7. At this prompt, run the following command:

```
/sbin/resetpw.sh
```

If successful, the **admin** password is now reset to an empty password. If any corruption of configuration state is detected, an attempt to save existing configuration databases is made and the system's configuration state is reset to initial values — i.e. the same state as when the system was manufactured. In this case, the **admin** password will be set to the 'empty' password. The command will notify you of any locations of saved configuration state.

```
sh-2.05b# /sbin/resetpw.sh
 Admin password reset successful.
 sh-2.05b#
```

8. The system can now be restarted by issuing the command **reboot** at the command prompt.

```
sh-2.05b# reboot
```

Web Interface

The platform configuration Web interface available on port 8003 provides the functionality described in the paragraphs below. After you have used the wizard to set up the WLM1200-RMTS's IP address, either manually assigned or assigned via DHCP, you can use the CLI to verify it, and then access this address using a browser.

To determine the IP address after it is assigned using DHCP, use the CLI command:

```
rm200a1 # show interfaces
Interface eth0 state
  Admin up:         yes
  Link up:          yes
  IP address:       172.21.26.231
  Netmask:          255.255.255.0
  Speed:            100Mb/s (auto)
  Duplex:           full (auto)
  Interface type:   ethernet
  MTU:              1500
  HW address:       00:30:48:33:43:E6
```

This shows you that the address is, in this example, 172.21.26.231. Using this address, you can connect to the appliance by entering:

https://172.21.26.231:8003.

The first screen displayed is the *RingMaster Platform Management Console* **Login** screen:

Enter the password, if any, and click on **Login**.

The *RingMaster Platform Management Console* provides screen in a hierarchy of tabs and items under these tabs: Each of these is described individually along with the Web browser screen.

Monitoring Tab

There are five items under this tab, as described below:

Summary Item

You first see the following screen. This screen provides a summary of the WLM1200-RMTS appliance, including information on the configuration and status.

CPU Load Item

If you click on **CPU Load**, you see the following screen showing CPU Load for the last hour and providing a button to click if you wish to **Pause** statistics collection. Clicking this button enables the **Resume** button.

Memory Item

If you click on **Memory** you see the following screen:

This screen also allows statistics collection **Pause** and **Resume** controls, and provides current memory statistics.

Network Item

Clicking on **Network** provides network usage statistics for both Ethernet interfaces.

File System Item

Clicking on **File System** brings up the following screen:

This screen provides last day disk usage, plus **config** and **var** disk partition statistics. **var** is the partition where all *RingMaster* application data is stored.

Setup Tab

There are fifteen items under this tab, as described below:

Interfaces Item

Clicking on **Interfaces** brings up the following screen:You can view and/or configure interface items on this screen.

Routing Item

You can view and/or configure static and dynamic routes and gateway on this screen.

DNS Item

You can view and/or configure domain items on this screen.

Hostname Item

You can view and/or configure system hostname and banners on this screen.

Changing the host name invalidates the currently installed license activation key.

Hosts Item

You can view and/or configure hosts on this screen.

Users Item

You can view user accounts and change passwords on this screen.

SNMP Item

Clicking on **SNMP** brings up the following screen:

You can view and/or configure SNMP and trap parameters on this screen

Faults Item

You can view and/or configure other fault reporting features on this screen.

Logging Item

Clicking on **Logging** brings up the following screen:

You can view and/or configure system logs on this screen.

Configurations Item

Clicking on **Configurations** brings up the following screen:

You can save the running configuration to the active configuration file, discard it, or reset both running and active saved platform settings to defaults on this screen.

Date and time Item

Clicking on **Date and time** brings up the following screen:

You can view and/or configure date and time values on this screen.

NTP Item

Clicking on **NTP** brings up the following screen:

You can view and/or configure NTP and associated servers on this screen.

Reboot Item

Clicking on **Reboot** brings up the following screen:

You can reboot or shut down the system on this screen.

Upgrade Item

You can view current or install new images on this screen. You can also revert to the previously active version. The system does not reboot itself as part of an upgrade. The upgrade sets up the standby partition. You must make upgrades effective by manually rebooting the system. If anything goes wrong during an installation procedure, the system resorts to running the previously active partition.

View Logs Tab

There are three items under this tab, as described below:

Continuous log Item

Clicking on **Continuous log** brings up the following screen:

You can view a continuous log on this screen.

Current log Item

Clicking on **Current log** brings up the following screen:

You can view the current log on this screen.

Archived log 1 Item

Clicking on any item **Archived log *n*** brings up a screen for that archive:

You can view archived logs on screens like this.

Backing up and Restoring WLM1200-RMTS Configurations

You can now configure the WLM1200-RMTS to automatically create backup files of current configurations and place them on external storage sites, an FTP or TFTP location. The files use the format *planname-date-time.zip*.

To configure this feature, follow these steps:

1. In the Auto-Backup Settings, select the interval for creating backup files from the Backup Interval list.
2. If you select Daily Backup, enter the time for creating the backup file in the Daily Backup Time fields.
3. Configure the number of backup files to create at the time of backup.
4. If you want to include the Monitoring Database, select Include Monitoring Database.
5. To transfer the backup files to a remote location, select Enable in the Remote Transfer section.
6. Select the type of transfer protocol.
7. Enter the URL of the remote location in the Remote Directory field.
8. If a username and password is required to access the remote location, enter the values in the Username and Password fields.

To transfer a backup file from a remote location to the WLM1200-RMTS, the following CLI command must be used:

```
rm-services download backup url
```

Configuring RADIUS Authentication for User Access

The WLM1200-RMTS can be configured to use RADIUS to authenticate users. Multiple servers can be configured and a default timeout value and default secret key can be configured for all RADIUS servers.

On the Setup page, configure the following parameters:

- Authentication Method List — you can configure up to three methods of authentication.
- Authorization — configure the role of the Default user.

On the RADIUS Configuration page, configure the following settings:

- Key
- Timeout
- Retransmit
- RADIUS Servers
- Add New RADIUS Server